The impact of AI on staff selection and recruitment

Organisations need to inform candidates when AI is used in recruitment. By **Paul McGrath**, **Pilar Arzuaga** and **Charlotte Moorhouse** of McDermott Will & Emery.

Artificial intelligence (AI) is increasingly being used by employers to help decide who they hire, whether that is from the initial screening stage all the way through to AI interviewing candidates and communicating with them throughout the recruitment cycle. Whilst there are obvious draws to leveraging AI to streamline recruitment processes in this way, there are also some important legal considerations for organisations using these tools to bear in mind. Most notably, these relate to data protection, cybersecurity and employment law compliance.

AI IN THE CONTEXT OF STAFF SELECTION AND RECRUITMENT

Preparing the job advertisements: Before the screening of candidates even begins, AI is being used in some instances to write or refine job descriptions and prepare advertisements for roles. Certain AI tools can reportedly track how different styles of language are received by different demographics, for instance, by identifying language that might discourage women and minorities from applying for roles. AI can then adjust the role advertisement literature accordingly to address these issues with a view to enhancing candidate engagement and attracting a diverse range of candidates applying for roles.

Screening: Traditionally, recruiters spent countless hours sifting through stacks of CVs. AI algorithms can now handle this task instantaneously by scanning all CVs received, extracting relevant information, and matching candidates to job descriptions. Candidates can then get ranked according to the job requirements and other qualification determiners.

This sort of automation naturally accelerates the initial screening process and allows recruiters to focus on more strategic aspects of the recruitment process. Using AI to blind screen candidates, ostensibly reduces the risk of human biases by relying on objective criteria (such as qualifications, skills, and experience) to evaluate candidates, without considering personal attributes like gender, ethnicity, age, or where the individual lives and/or was raised.

Interviewing: After the initial screening process, candidates may be required to participate in an assessment or attend an interview. AI is increasingly being used to (a) interview candidates with pre-set questions; and (b) analyse the answers given in these interviews. For example, various algorithmic models measure the quality of a candidate's answer against similar responses and process thousands of responses quickly to look for specific words or language that reflect the values of the employer. Candidates are then ranked in order of their strength and compatibility for the role.

AI now even has the capability to assess softer skills in candidates. For instance, AI video-interviewing systems can examine speech patterns, tone of voice, facial movements and other biometric indicators to provide an insight into a candidate's style of non-verbal communication.

Tracking the process: The use of Applicant Tracking Systems (ATS) is also growing in popularity. ATS powered by AI helps streamline the entire recruitment workflow. It can manage candidate data, track progress, and facilitate communication. Recruiters can easily access candidate profiles, interview schedules, and provide feedback all in one place.

Practical issues with AI technologies

Transparency issues: Many AI algorithms currently operate as "black boxes", meaning their decision-making processes are not easily explainable or interpretable.

This potential lack of transparency can make it challenging for employers to understand how the system reached a specific conclusion, raising concerns about accountability and fairness. In turn, this potentially limits an employer's ability to articulate to candidates why they have been unsuccessful in an application process.

AI biases: Depending on the underlying algorithms of the particular AI tool being used and how it is deployed, AI systems can themselves potentially give rise to bias. This can include, for instance, where the AI is reliant on learnings acquired from real-world data that itself included examples of human biases; AI could potentially reaffirm and exacerbate these biases.

Human touch: Recruitment of staff is, at its core, a people process. Overuse of AI at this critical early stage in the relationship with a prospective new hire has the potential to negatively impact the candidate's experience and may therefore lead to disengagement and/or withdrawals from recruitment processes.

Key legal considerations

There are currently no specific laws that explicitly regulate the use of AI in a recruitment or wider workplace context. There are, however, a number of existing statutory and common law principles that impact how these emerging AI technologies can lawfully be used by employers in selection and recruitment (and, indeed, the wider workplace context).

Data protection: Organisations leveraging AI within HR must navigate the intricacies of the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), which sets stringent guidelines around the processing of personal data. Central to data protection law compliance is the principle of lawful processing. Organisations using AI systems to process candidate or employee information must identify a permissible legal basis for this activity. For instance, depending on the nature of the data at hand, this can include legitimate interest, contractual necessity or (as will most often be the reason relied on in the context of recruitment) express and informed consent.

The UK GDPR requires prospective employers to notify candidate data subjects about their personal data handling practices through a privacy notice at the time such data is collected. Amongst other things, this includes providing information about the existence of any automated decision-making (and, where such automation is used, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the candidate). It is therefore important that employers understand how the AI tools they are using work, what they do and don't do, and can explain this coherently to candidates.

In addition to a comprehensive candidate privacy notice, a second pivotal aspect of compliance in this area is for an employer to conduct a Data Protection Impact Assessment (DPIA) before deploying any AI technology. DPIAs allow organisations to identify and mitigate risks to the privacy and rights of data subjects.

Alongside DPIAs, organisations must implement appropriate technical and organisational measures to safeguard data, guided by the Information Commissioner's Office (ICO). The ICO offers specific guidelines on AI and data protection, delineating best practices for UK GDPR compliance within the context of AI. Other data protection compliance principles must also be adhered to, such as data minimisation.

In the usual way too, candidates are, as data subjects, entitled to access, from the data controller employer deploying AI technologies to any personal data that has been processed, to request rectification and/or erasure, and to object to processing. The design of AI systems must, therefore, facilitate the exercise of these rights, embodying transparency and accountability.

Cybersecurity: As in all cases where technology is used to process personal and other confidential data, robust cybersecurity measures should be adopted to protect against data breaches and cyber threats. The underlying laws in this area anticipate that organisations will adopt a comprehensive approach built on the principles of secure coding and privacy by design.

Ongoing efforts to maintain AI system security are also crucial. Regular software updates and patches addressing emerging vulnerabilities, together with continuous monitoring, should form the backbone of a broader vulnerability management programme. Security audits and penetration testing, conducted by qualified professionals can be used in addition.

Third-party due diligence may also assist organisations in assessing the technical viability of potential new AI tools.

Other practical measures that should be taken reflect best practice from other areas of data handling and include:

- Ensuring that access to data is restricted to only those individuals who need to access it for the purpose it was collected;
- Adopting strong sign-in and authentication checks;
- Implementing a policy about who can access the data and permitted uses of that data;
- Keeping track of who does what with the data; and
- Training all those involved on the use of the systems and cybersecurity.

Equality and anti-discrimination laws: The Equality Act 2010 imposes legal duties on employers to avoid unlawful discrimination against prospective employees during the recruitment process on the basis of any protected characteristic.

Protected characteristics include age, gender reassignment, marital or civil partnership status, being pregnant or on maternity leave, disability, race

including colour, nationality, ethnic or national origin, religion or belief, sex and sexual orientation.

Importantly, liability for any unlawful discrimination will fall on the prospective employer, regardless of whether the recruitment process and/or decision making was driven by a human, or any AI assisted technology. This is therefore an added reason for employers to understand how the AI tools they are using work, and to be able to describe and account for the determinations they make. Outputs from AI tools being deployed ought to be regularly audited by humans for any potential bias.

The risk of discrimination is not just limited to direct discrimination (less favourable treatment based on a protected characteristic). Using AI tools in recruitment could also conceivably be considered to be a "provision, criterion or practice" which could give rise to claims of indirect discrimination if it places one or more protected groups at a particular disadvantage without objective justification.

In addition, a duty to make reasonable adjustments to the manner in which AI tools are deployed could apply requiring prospective employers to remove potential disadvantage that may be suffered by disabled applicants.

Mutual trust and confidence: The relationship between an employer and employee is founded on a high degree of mutual trust and confidence. To that end, the common law implies a term into all employment contracts that an employer will not without reasonable cause conduct itself in a way calculated or likely to destroy or seriously damage that trust and confidence. This principle is so fundamental to the relationship that an employee may treat themselves as constructively dismissed if breached.

Whilst this principle only applies to employees and not prospective employees, and will not therefore apply to all job applicants, it will be of relevance when considering internal applications by existing employees (such as promotion opportunities).

Privacy: Some AI tools may search for information on candidates and/or employees which has not readily been provided by the individual through the application process.

Article 8 of the European Convention on Human Rights provides that everyone has the right to respect for their privacy. This applies to employees, workers and prospective employees. This right can, in principle, extend to protections against workplace monitoring by an employer.

Employers therefore have a duty to ensure that AI technologies do not unduly infringe upon individuals' privacy rights.

Key takeaways and best practices

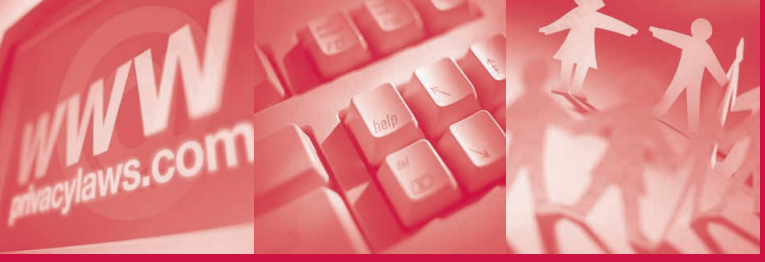
1. Organisations are required to inform candidates when AI is utilized in the recruitment process and must have a lawful basis for processing personal data in this manner.
2. Compliance with the Data Protection Act 2018 and the UK GDPR is mandatory for organizations using AI in recruitment. This includes adopting the security measures specified in Article 32 of the UK GDPR, such as encryption, pseudonymization, and ensuring the continuous confidentiality, integrity, availability, and resilience of processing systems.
3. Adhering to the Network and Information Systems Regulations 2018 (NIS Regulations) is essential for certain organisations. These regulations mandate the reporting of significant cybersecurity incidents, underscoring the need for high security across all network and information systems, including those involved in AI-driven recruitment.
4. Engaging in proactive risk management through regular security assessments and third-party due diligence is crucial for identifying and mitigating vulnerabilities within AI systems.
5. While AI can greatly improve the efficiency of candidate screening, it may not fully grasp complex human subtleties, potentially leading to discriminatory outcomes. To address this point, it is vital for employers to conduct DPIAs when deploying AI tools. DPIAs help identify and mitigate any risks related to data protection and privacy, including potential biases or discrimination.
6. A comprehensive privacy notice is crucial for data protection compliance. Employers are obliged to provide clear and comprehensible explanations for decisions made by AI and automated processes.
7. Strong cybersecurity measures are imperative to safeguard personal data, and the AI tools employed must adhere to equally stringent security protocols.
8. Regular audits of AI tools and decisions are crucial to uncover and rectify any issues, ensuring fair and equitable treatment of all candidates. Employers will be held accountable for discrimination claims, irrespective of whether decisions about a candidate were made by an AI tool or a human. As such, it is important to frequently audit recruitment decisions to check for any potential biases.

AUTHORS

Paul McGrath is a Partner, Pilar Arzuaga a Senior Associate and Charlotte Moorhouse an Associate at McDermott Will & Emery UK LLP.
Emails: Pmcgrath@mwe.com
parzuaga@mwe.com
Cmoorhouse@mwe.com

REFERENCE

1 www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018



ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Spotlight on cookies: An increased regulatory focus

As the ICO warns organisations that use advertising cookies, **Emma Erskine-Fox** of TLT advises on how to ensure cookie compliance and avoid regulatory action.

The rules on cookies may not have substantively changed since 2011, but regulatory guidance has significantly evolved in the last few years, addressing concerns with increasingly intrusive uses of these technologies to track individuals and send them ads.

Recent developments have brought this issue, previously seen as a low-risk area, to the forefront of many organisations' and privacy

Continued on p.3

AI and ADM: No transparency and no choice?

Alexander Dittel of Wedlake Bell LLP discusses how privacy notices should address the processing of personal data relating to machine learning, artificial intelligence and automated decision-making.

As transparency and choice are two of the essential principles of data protection law, their implementation in relation to AI and ADM raises several issues. These challenges are similar to those encountered in training machine learning (ML) models over the last ten years.

The large-scale collection of public data for the training of ML/AI models is at the core of this discussion. The

Continued on p.5

Issue 132 **MARCH 2024**

UNITED KINGDOM
report

ISSUE NO 132 **MARCH 2024**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Emma Erskine-Fox
TLT LLP
Alex Dittel
Wedlake Bell LLP
Sally Annereau
Taylor Wessing LLP
Paul McGrath, Pilar Arzuaga and Charlotte Moorhouse
McDermott Will & Emery LLP
Rebecca Cousin, Lucie van Gils and Ian Ranson
Slaughter and May
Katie Hewson, Daniel Jones and Nelson Kiu
Stephenson Harwood LLP
Richard Field
Appleby

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

UK to legislate on advanced AI 'when the time is right'

The UK aims to be a Science and Technology Superpower by the end of the decade. The government continues to believe that a light-touch regime is the best way to achieve this aim – in stark contrast to the EU's world-leading new AI Act. Issuing its response to the AI White Paper consultation on 6 February, the government also announced a £100 million package to help realise new AI innovations and support regulators' work on AI. The government says this will help them to develop cutting-edge research and practical tools to address AI risks.

The government says it will not want to rush into legislating before it fully understands the risks and opportunities of AI. "However, the challenges posed by AI technologies will ultimately require legislative action in every country once understanding of risk has matured." Therefore, legislation may in time be introduced for highly capable GenAI.

For now, the government continues on its pro-innovation path asking existing regulators to apply cross-sectoral principles. Regulators will need to outline their strategic approach to AI by 30 April 2024.

In the meantime, organisations need to tackle practical problems such as revising privacy notices in light of using AI and automated decision-making p.1). AI is also a game-changer in staff selection and recruitment (p.12). Amongst all the challenges, we can celebrate the renewed adequacy decisions for Guernsey (p.21), Jersey and Isle of Man, and the modest reliefs to companies' subject access compliance burden, as proposed in the Data Protection and Digital Information Bill (p.10).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"Given the rate of change in law, regulation and business practice, it is essential to have concise and up to date information. *PL&B* is always relevant and continues to offer great value.."

Adam Green, Chief Risk Officer, Equiniti

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 37th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.