YOONO

Stay in the Know with YOONO

The Legal Landscape of AI in Recruitment

YOONO Insight: VOL 1


YOONO

Contents

Preparing for the future of recruitment

The world of recruitment is rapidly changing. Artificial Intelligence (AI) is introducing convenience, efficiency and data-assisted intelligence into the background screening process, but alongside these exciting developments, many businesses are anxious about the legal risks, and unsure how to ensure AI remains a compliant part of their hiring practices.

This technology will no doubt revolutionise recruitment, in the same way it is revolutionising other industries. What we want to provide at YOONO is the complete picture for our customers, so that you can be fully informed when using data-powered screening in your own business.

This booklet aims to demystify core topics and issues surrounding AI background screening, with the direct advice of YOONO's Chief Legal Officer, James Clark. James will address key concerns in this area, including data protection (GDPR), bias and ethical considerations, so you can be aware of key legal advice before adopting AI into the way you hire.

James Clark

Chief Legal Officer at YOONO

James is Chief Legal Officer at YOONO, bringing his experience with advising on multiple aspects of data law to help YOONO deliver a fully-compliant service for customers. A specialist in demystifying complex areas of data law, including data protection legislation, artificial intelligence application, human rights and cyber security, James has previously worked within global law firm DLA Piper, focussing on multiple international projects in the UK, Brussels and Washington, D.C. A highlight of James' career to date was his role advising the UK government's Office for AI on the future of AI regulation in this country. He also speaks and writes about data protection for a number of known publications.

As the author of this white paper, James brings his wealth of experience and expertise to the subject of AI in recruitment, to help you make an informed decision for your business.

About YOONO

YOONO provides thorough background intelligence about job-seeking candidates. Recruiters can generate customised reports about an individual and assess their suitability for a role.

YOONO is a next-generation background screening tool that aims to preserve company reputation, while cutting research time and costs. Quick and intuitive to use, YOONO processes publicly-available data using cutting-edge AI tech, allowing users to remain compliant within data privacy guidelines.

What we want to provide at YOONO is the complete picture for our customers,

so that you can be fully informed when using data-powered screening in your own business.

Introduction: The AI recruitment revolution

It is no exaggeration to say that the world of recruitment—and the world at large—is experiencing an AI-powered revolution. The uptake in the use of AI tools by recruitment teams has been seismic, with an estimated 87% of organisations now using AI at some stage in their hiring process.[1]

For many reasons, this is not surprising. Hiring managers and recruitment teams experience increasing pressure to review and compare information about candidates, and to make difficult decisions about screening, progressing and ultimately selecting successful ones.

In this digital age, the amount of information that is available

87%

of organisations now use AI in their hiring process

about candidates can be daunting at best, if not completely overwhelming. In this context, AI tools do seem like the perfect solution—engineered to automate the review of large quantities of information, and capable of comparing candidate CVs using objective and data-driven methods. Busy recruitment teams understandably want the extra support, insight and efficiency that AI tools can offer.

However, alongside the surge of interest in recruitment-based AI tools comes a rise in regulatory scrutiny.[2] Data protection, employment and equality laws all wield influence in the field of recruitment AI, and both regulators and courts have demonstrated an interest in ensuring that these tools are used responsibly, and that candidates do not face unfair discrimination.

Consequently, businesses are advised to proceed with an informed perspective, and to fully understand the legal landscape before choosing to use AI as part of their recruitment process. As we'll look at in this paper, it is perfectly possible to use AI tools safely, responsibly and in compliance with the law, as long as businesses are mindful of certain risks and relevant measures are adopted by both the employer and by the provider of the AI tool.

[1] https://www.demandsage.com/ai-recruitment-statistics/
[2] See, for example, the ICO's project to audit some of the most popular AI tools used in recruitment: https://ico.org.uk/action-weve-taken/audits-and-overview-reports/ai-tools-in-recruitment/

It is perfectly possible to use AI tools safely, responsibly and in compliance with the law,

as long as businesses are mindful of certain risks and relevant measures are adopted by both the employer and by the provider of the AI tool.

How does UK and EU law apply to AI screening tools?

The UK does not currently have any AI-specific laws. Instead, the development and use of AI tools is indirectly regulated by a range of legal frameworks. In the context of recruitment, the most relevant legal frameworks for a user of AI tools are:

Data protection law

(GDPR)

Employment law

in particular equality and anti-discrimination obligations

The EU has passed one of the world's first AI-specific laws, known as the AI Act. The AI Act is being introduced in stages, with most of the key provisions becoming effective in the near future, in August 2026.

Although the UK is no longer an EU Member State, the AI Act has 'extraterritorial effect', meaning that it will still apply to UK companies in certain circumstances. For example, in a recruitment context the AI Act is likely to apply where a UK company is using an AI tool to help make decisions about EU based candidates.

In addition to the strict letter of the law, the use of AI in recruitment is heavily impacted by ethical and reputational concerns. Businesses normally want to be recognised for running friendly and fair recruitment processes, and to avoid any implication that they are using technology in a way that does not align with their corporate values.

Key data topics recruiters should know about

GDPR and data protection

All AI tools are built on and around data—they process large volumes of data, which are fed through one or more algorithms in order to produce an 'output'. This output might be a recommendation, a decision or some other piece of text, such as a summary. Where that data includes 'personal data', which is information that relates to an identifiable person, then data protection law becomes engaged.

Most of the obligations under data protection laws (which, in the UK, are principally the UK GDPR and the Data Protection Act 2018) apply to the 'data controller', who is the person making decisions about how and why personal data is used.

In the context of a recruitment process, the data controller is the employer.

What are data protection principles?

At the heart of data protection law are the data protection principles. These are a set of baseline requirements that are applicable to all uses of personal data, including in the context of an AI screening tool.

Interestingly, there is significant overlap between the data protection principles and widely acknowledged principles for the safe and ethical use of AI[3]. In other words, ensuring that you comply with the data protection principles is a good way of also ensuring that your use of AI adheres to accepted standards. Know the principles, and stay compliant!

The data protection principles apply to AI tools as follows:

Fairness, lawfulness and transparency

Users of AI tools should ensure that personal data is processed fairly by AI tools, and that AI tools do not produce unreasonable or unexpected outcomes. A 'lawful basis' (such as consent, performance of a contract or legal obligation) must be established for each activity performed by the tool that uses personal data. Finally, users must be transparent and open with individuals about how and why their AI tool processes personal data. Read a little more about transparency below.

[3] See, for example, the OECD AI Principles: https://www.oecd.org/en/topics/ai-principles.html

Purpose limitation

Personal data collected by an AI tool should be used for a clearly defined purpose (such as screening candidate CVs) and should not be re-used for additional, unrelated purposes. That purpose should be one that the AI tool is designed to perform.

Data minimisation:

Organisations should only collect the minimum amount of personal data that is required for the AI tool to perform its defined purpose.

Storage limitation:

Personal data subsisting in the output of an AI tool (such as a written summary or report) should be kept for no longer than is necessary for the defined purpose.

Integrity and confidentiality:

The rules of information security apply to AI tools. Where these use personal data, they should be accessible on a need-to-know basis, and any unauthorised access, alteration or loss of data may need to be dealt with as a personal data breach.

Accuracy:

Organisations should take reasonable steps to ensure data processed by an AI tool is accurate and up to date. Here, the 'garbage in and garbage out' maxim of computer science applies—keep in mind that the outputs of the AI tool will only be as good as the data that is fed into it!

Accountability:

Organisations must be accountable for their use of personal data in AI tools. Amongst other things, this means maintaining and enforcing written policies on the use of AI tools and the protection of personal data, as well as providing training and direction to staff.

What is a privacy notice?

Any organisation that processes personal data must provide a notice to data subjects that explains how and why their personal data is used, and the rights available to them under data protection law. This is typically referred to as a privacy notice (or privacy policy).

Where an AI tool processes the personal data of candidates, the notice obligation also applies. As a result, organisations must ensure that the use of their AI tool, including the specific purpose for which it is used, is covered by their privacy notice. For example, if the tool is used to build an automated profile of the candidate, based on factors such as their demographics, past behaviours or work history, this profiling activity must be specifically addressed in the notice.

Candidate clarity about automated decision making

A particular risk arises under data protection law where an organisation uses an AI tool to make an 'automated decision' about a candidate. Individuals have a legal right not to be subject to automated decisions that result in legal or other significant effects, other than in limited

circumstances, and subject to certain legal rights.

If a business relies solely on an AI tool to take a decision about whether to offer someone a job (sometimes termed 'robo-hiring'), it is likely they are engaging in automated decision making. To remain compliant, this needs to be clearly explained to candidates - see What is a privacy notice? above, and individuals need to be informed that they have the right to:

Receive meaningful information about the logic used by the AI tool

Express their point of view about the decision

Obtain human intervention into the decision

Ultimately, be able to contest the decision

Often, the judgment about whether an AI tool is being used to actually make a significant decision, or merely to support the decision making of a human being (such as a hiring manager), is a nuanced one, that requires careful analysis and action.

Other data subject rights

Candidates also have other data subject rights under GDPR guidelines. This includes the right to access personal data held about them by an organisation, including any personal data used or produced by an AI tool, as well as the right to demand the deletion of personal data, in the scenario where an organisation cannot demonstrate a lawful reason to retain and use the data.

The role of governance (DPO and DPIAs)

As with all activities involving the processing of personal data, the use of an AI tool should be subject to the oversight of the organisation's data protection officer (DPO), where a DPO has been appointed.

Further, depending factors such as the purpose for which the AI tool is used (in particular, whether it is used for automated decision making), the sensitivity of the data processed, and the novelty of the technology, it may be necessary for the organisation to conduct a data protection impact assessment (DPIA) prior to deployment of the AI tool.

Key data topics recruiters should know about

Employment and equality law

From an employment law perspective, it is important to consider compliance with the Equality Act 2010, which prohibits organisations from unwarranted discrimination on the basis of protected characteristics such as age, sex, race, disability, and other factors. AI tools must be carefully managed to ensure that they do not themselves take discriminatory decisions, or do not provide recommendations to hiring managers that result in discriminatory decisions.

There is concern that some AI systems may inadvertently replicate historic biases present in their training data. For example, if an AI tool has been trained predominantly on recruitment applications from candidates of a particular background, it may not view applications from minority candidates as favourably, or be equipped to interpret them as accurately. If hiring managers themselves have latent biases, the AI tool may in turn compound these biases.

This is why it is extremely important to select and use an AI tool that has been developed with bias mitigation in mind, with YOONO as an example of a screening tool that has been designed around neutral algorithms.

The employer's ability to influence the training of an AI tool may be limited, which underscores the importance of careful supplier due diligence, and obtaining appropriate assurances from AI tool providers about their model training and testing processes. If providers are subject to the AI Act (see below), then they will be required to produce documentation explaining these processes, as well as how-to manuals to guide the companies who use their tools.

The common law imposes a duty of mutual trust and confidence between employers and employees. Consequently, where a AI tool is used to process data of current employees, as an example, for an internally advertised vacancy or a promotion decision, employers will have an obligation to ensure that their use of the AI tool is fair and reasonable, and that transparency regarding the use of the tool is carefully considered.

In support of the general principles of the common law and good practice more broadly, the government's Responsible AI in Recruitment Guidance[4], for instance, recommends practical measures such as conducting impact assessments, continuous monitoring, and ensuring robust appeal processes for candidates affected by AI-driven decisions.

[4] Responsible AI in recruitment - Guidance:
https://assets.publishing.service.gov.uk/media/65fda1b9f1d3a0001132ae5b/Responsible_AI_in_Recruitment.pdf

Key data topics recruiters should know about

The AI Act

The EU AI Act is a risk-based law that came into force on 1 August 2024. It seeks to regulate, above all, so-called 'high risk AI systems'. Unfortunately for UK employers that have operations in the EU, the use of an AI tool for candidate selection or evaluation is regarded as high risk for these purposes.

The Act distinguishes between the provider and deployer of an AI system, with the majority of obligations falling on the provider—that is, the company that develops the AI system and puts it on the market. Therefore, unless the employer has developed the AI tool in-house, then most of the AI Act compliance burden is likely to lie with the supplier of the tool.

However, the employer will still need to take steps to validate and obtain contractual assurance regarding the supplier's compliance with the duties of a provider under the Act. These duties include:

- **Performing comprehensive risk assessments**
- **Implementing robust risk management and conformity assessment procedures**
- **Preparing detailed technical documentation**
- **Monitoring post-market performance**

As the deployer of a high-risk AI system, an employer using an AI tool in a recruitment context will need to:

- **Ensure the AI tool is used strictly in accordance with the provider's instructions**
- **Assign competent personnel to exercise active human oversight**
- **Provide AI literacy training to staff**
- **Continuously monitor the system's performance, and document and report any performance issues to the provider**

Are AI rules becoming more enforced?

In recent years, we have seen an increase in regulatory action relating to AI tools, as well as a growing trend for individuals to use the courts to enforce their rights and challenge unfair uses of those tools by employers.

The Information Commissioner's Office (ICO), which is the UK's data protection regulator, has made the use of AI tools in recruitment one of its key areas of focus in recent years.

Following an expansive audit of AI tools conducted in 2024, the ICO produced a detailed outcomes report,[5] as well as specific guidance for organisations using those tools.[6]

The ICO has also shown itself willing to take enforcement action in the context of AI more broadly, including in the cases of Snap and Clearview AI.

An interesting example of employers being challenged in the courts for their use of AI tools can be found in the cases brought against ride-hailing service Uber by UK-based Uber drivers. Represented by their union, the drivers challenged Uber over its use of automated decision making, in cases where drivers were dismissed based on algorithmic assessments. In an example of 'robo-firing' practices being challenged in the courts, the drivers alleged that Uber did not comply with GDPR when dismissing drivers flagged as engaging in alleged fraudulent activity by an AI tool. The drivers argued that Uber had not been sufficiently transparent in its use of the AI tools, and had not provided drivers with the right to challenge automated decisions.

Whilst both regulatory enforcement and litigation risks exist, the most relevant challenge for the majority of companies will be the practical risk of disruption, caused by informal challenges and complaints brought by unsuccessful candidates who distrust an employer's use of AI tools. Such candidates may also look to use social media and other public platforms to voice their grievances, which may impact on business reputation and PR strategy.

[5]chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ico.org.uk/media/about-the-ico/documents/4031620/ai-in-recruitment-outcomes-report.pdf
[6]https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/thinking-of-using-ai-to-assist-recruitment-our-key-data-protection-considerations/

5 ethical AI principles to know and observe

In the UK, the government has set out five basic principles that it believes should apply to the use of AI.[7] Having these principles at the forefront of your organisation's approach to AI governance will help to alleviate ethical concerns that candidates might otherwise have about the use of AI.

In addition to these principles functioning as a 'yardstick' for companies to follow, they are also the core principles that regulators (including the FCA, the ICO and the CMA) have been told to consider when monitoring the use of AI within their domains.

Below you can find the UK principles, alongside some of the steps that we often see organisations taking in order to adhere to them in practice.

[7]chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d0013c821a0/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf

1

Safety, security and robustness:

AI tools should comply with prevailing laws and regulatory standards (such as the AI Act), and should have been properly tested to function accurately and safely for the proposed use case. Organisations should ensure that AI tools are made available on a need-to-know basis, and that data is kept secure and confidential, where appropriate.

2

Transparency and explainability:

It's clear that many ethical concerns surrounding AI are exacerbated by a lack of transparency. Candidates are more likely to object to the use of an AI tool (or find it 'creepy'!) When they think it has been deployed in an underhand way, without adequate explanation about how the tool is used, and how it influences the recruitment process. In most cases, the reality of how the tool is used will be much less concerning than a candidate's worst fears, and so it's generally best to simply be clear and upfront. In addition, organisations need to be able to explain, in basic terms, how an AI tool functions and how it has produced its recommendations or decisions.

3

Fairness:

Organisations can ensure that the AI tools they use are, as much as possible, free from 'trained bias' and that datasets used to train the tool are representative of the population on which they will be used. It's also advisable to use the AI tool for a purpose for which it was designed. Companies can also take steps to supervise the AI tool and override any unfair recommendations or decisions.

4

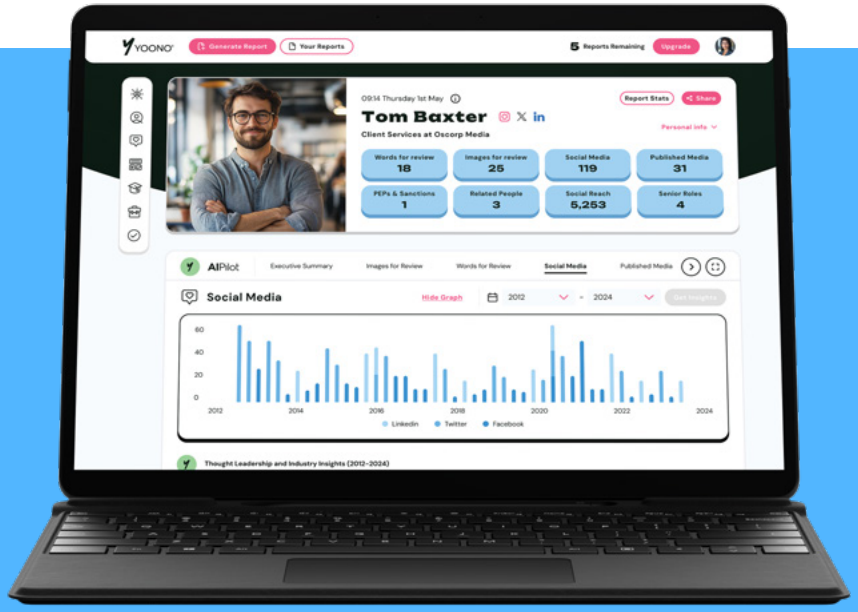
Accountability and governance:

How the tool should be used is to be documented, and appropriate AI literacy training provided for staff. Keep track of any errors produced by the tool, so that these can be reported and technical fixes performed. Ensure that the organisation has escalation mechanisms in place to oversee the use of AI and help to resolve any disputes.

5

Contestability and redress:

Mechanisms should be provided to allow impacted individuals to challenge decisions made by AI tools, obtain more information about how the tool has impacted a particular process, and ultimately to request human review of the tool's output.



In the UK, the government has set out five basic principles that it believes should apply to the use of AI.

Having these principles at the forefront of your organisation's approach to AI governance will help to alleviate ethical concerns that candidates might otherwise have about the use of AI.

A note from YOONO

Empowering businesses to recruit with confidence

In this white paper, James has outlined the evolving (and sometimes complex) legal landscape of AI. AI presents many exciting possibilities for the recruitment industry, but it is also important to be aware of the legislation and best practice for using these innovative forms of technology, to avoid introducing unfairness, bias or discrimination into your hiring process, and to reduce the risk of legal challenge by candidates or regulators.

As we move forward into this new era of recruitment, it's clear that both organisations and AI providers must strike an ethical balance. On the one hand, the advantages of using AI are extremely clear, and businesses which don't adopt the technology may risk being rapidly left behind as progress in this area continues to revolutionise

recruitment. On the other, it is possible that AI can be used—consciously or not—in a way that is unfair to candidates, and that introduces unwanted legal risk into the hiring process.

This is why it is paramount that organisations use AI tools that place ethical and legal considerations front and centre. Background screening service YOONO prides itself on offering a responsible AI product, where compliance with these laws has been considered at all stages of product design. Focused solely on publicly available data, YOONO is able to provide a transparent intelligence service that differs from its competitors. YOONO is also committed to ensuring that its customers are informed about the legal landscape of AI, and the responsibilities that they have as the users of an AI product.

We hope that this white paper has helped to demystify some of the complicated topics and issues surrounding AI in recruitment, and that it will serve as a useful resource to share with your colleagues. Stay ahead of the game, and step into the future of recruitment from an informed perspective.

Discover
the future of
recruitment