MEALEY'S® LITIGATION REPORT:

Artificial Intelligence

The Future Of Work: Exploring The Employment And Data Protection Law Implications Of The Use Of Artificial Intelligence (AI) In European Workplaces

By
Matthew Howse,
Louise Skinner,
Vishnu Shankar
and
William Mallin

Morgan Lewis
London, England

A commentary reprinted from the December 2024 issue of Mealey's Litigation Report: Artificial Intelligence

Commentary

The Future Of Work: Exploring The Employment And Data Protection Law Implications Of The Use Of Artificial Intelligence (AI) In European Workplaces

By
Matthew Howse,
Louise Skinner,
Vishnu Shankar
and
William Mallin

[Editor's Note: Matthew Howse, Louise Skinner and Vishnu Shankar are Partners and William Mallin is an Associate in the London office of Morgan Lewis. This article is provided as a general informational service and it should not be construed as imparting legal advice on any specific matter. Any commentary or opinions do not reflect the opinions of Morgan Lewis or LexisNexis®, Mealey Publications™. Copyright © 2024 by Morgan Lewis. Responses are welcome.]

Employers are increasingly integrating AI-driven tools across a wide range of functions. The deployment of AI in workplaces will undoubtedly change the current working landscape, redefine how workplaces operate and potentially introduce a wide range of new opportunities. However, the use of AI systems in the workplace is not without legal risk. This article explores some of the key employment and data protection law implications surrounding an employer's use of AI, as well as the ramifications of the new EU AI Act on an employer's deployment of AI systems.

Employment Law Considerations

AI has many use cases in the workplace and throughout the employment lifecycle. These include applicant screening, sourcing, interviewing and selection, determining promotion and termination decisions, and supporting fingerprint and/or face scanning biometrics for access to business premises. While the UK does not currently expressly regulate the use of AI in an employment context, there are existing areas of UK legislation and common law that can restrict an employer's use of AI in practice. We examine below the key risk areas in this context, namely discrimination, and unfair and constructive dismissal, as well as certain practical points for employers to consider.

Discrimination

The primary employment law risk to consider in this context is potential discrimination. The UK's principal anti-discrimination laws are found in the Equality Act 2010 (**EqA**). The EqA prohibits various forms of discrimination, including direct discrimination, indirect discrimination, harassment and victimisation based on nine legally protected characteristics (e.g., sex, race and disability). The discrimination risk exists because AI tools can exhibit biases that may impact decision-making if no checks and balances are implemented. The discrimination threat is potentially significant because not only can AI-enabled tools convey human bias in the way that they are operated, but they can also reproduce inequalities that are baked into the code and data sets themselves.

By way of example, certain AI-face recognition technologies have allegedly discriminated against individuals based on their ethnicity and gender, as there is evidence that such tools can misidentify, or are less reliable in respect of, people of certain races and genders. In particular, research suggests that face recognition software is less effective in correctly identifying black women's faces than white men's. AI-driven systems may also indirectly discriminate by failing to take certain contextual factors into account when making decisions regarding individuals' employment status, which would otherwise be obvious to a human. It is possible, for example, that an AI shift allocation tool which uses data to allocate shifts (and therefore pay) to workers may offer reduced shifts to an employee who is disabled or not able to work on certain days of the week. Similarly, an algorithm that is designed to make promotion decisions may well be designed to be gender blind but could nonetheless be indirectly discriminatory if it factors in average working hours into its assessment of work performance. This is because statistics show that women disproportionately have greater caregiving responsibilities and are therefore more likely to work less hours and/or work on a part-time basis. Employers using AI-driven applicant screening tools will also need to consider whether the programme employs data from its own workforce to determine whether an individual is a good fit for the business, and the extent to which this may perpetuate ongoing inequalities in its own workforce if, for example, its existing workforce is male dominated.

To mitigate against the potential discrimination risk, employers should ensure that there is human oversight of such processes. It is recommended that managers have final responsibility for any decisions that could have significant impacts, including regarding hiring, pay, promotions and the potential for dismissal. Further, consideration should be given to having HR teams and managers trained on how to understand algorithms and interpret any resulting data, including checking the accuracy of the data relied upon and implementing policies around the use of AI tools.

Unfair and constructive dismissal

Beyond discrimination, there are also potential risks of unfair and/or constructive dismissal claims due to the use of AI systems. In the UK, employees with over two years' service benefit from protection against ordinary unfair dismissal. To mitigate against the risk of unfair dismissal claims, employers must show that the employee was dismissed for one of the five potentially fair reasons as set out in the Employment Rights Act 1996. The employer must also act reasonably in treating that reason as sufficient for dismissal. Where an employer uses an AI system to make decisions as to whether an employee ought to be dismissed, it may be more challenging to explain or justify the basis for the decision, and to satisfy an employment tribunal that a fair procedure had been undertaken. This could particularly be the case where the employer is using a third-party AI system which it did not develop itself and therefore may not have sufficient knowledge of how the system actually operates in practice. It is possible that an AI-driven tool may issue and/or recommend a termination decision that is not underpinned by one of the five potentially fair reasons. Accordingly, human oversight over this process is crucial, as well as appropriate due diligence at the outset as to whether unfair dismissal compliance is built into the applicable software. Further, to ensure that meaningful consultation can take place, it is recommended that the relevant decision-maker ensure that they have an adequate understanding of the AI-system and how any dismissal decision was undertaken such that this can be properly explained to the employee.

An employee is constructively dismissed where they resign in response to an employer's repudiatory breach of contract. A typical example of a repudiatory breach of an employment contract is the breach of the implied term of mutual trust and confidence. The implied duty prevents an employer from acting in a way which would destroy or seriously damage the relationship of trust and confidence between employer and employee without reasonable and proper cause. Where AI-enabled systems are used to make important workplace decisions, employers must bear in mind that employees may consider that an AI system has not acted rationally, lawfully and/or in good faith, and the potential opaqueness of such decisions should be addressed prior to deployment by employers through transparent communication.

Practical considerations

At a practical level, the improper use of AI systems by employers can undermine the trust between an employer and their staff, owing to the "black box" nature of AI-driven technologies from an employee's perspective. Employers looking to harness AI in their workplaces are well advised to be upfront with staff and explain the rationale for the integration of such technologies into their HR practices and what guardrails are put in place to make sure AI is used appropriately. Moreover, in their due diligence of the software provider, it is recommended that employers carefully consider at the outset of any procurement process whether they fully understand the solution being provided and what steps are taken to ensure compliance with applicable law. One further practical point for employers to consider in this context is the mechanism for ensuring that the AI-tool provider will cooperate with the employer in any litigation process. Employment tribunal disclosure processes will likely be more complicated where decisions have been based on algorithms owned by third parties, and there are also important liability issues to consider and potentially address in contracts between the parties.

Data Protection Considerations

The use of AI during the employment lifecycle will almost inevitably involve the processing of personal data. A key operational benefit of AI lies in its ability to generate and process vast amounts of data in short periods of time. However, employers must be mindful of their obligations under the EU and UK GDPR (**GDPR**), as well as all applicable domestic data protection and cybersecurity laws. As with all forms of personal data processing, organisations will have to consider relevant data protection obligations when using AI systems. This may include identifying and documenting the appropriate lawful bases for such personal data processing, assessing whether their data protection notices need updating to reflect the use of AI tools and the data processing provisions and, where necessary, the international transfer safeguards, entered into within their commercial contracts with third-party providers of AI-enabled systems. For the purposes of this article, however, we touch on a few of the more notable data protection implications arising out of the use of AI specifically in a workplace context. These topics are solely automated processing, data protection impact assessments (**DPIAs**) and rights of access.

Solely automated processing

The GDPR contains specific provisions concerning so-called "solely" automated individual "decision-making" involving personal data, including profiling. According to article 22(1) GDPR, individuals have the right not to be subject to a "decision based *solely* on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them – unless an exemption set out in the GDPR or EU member state or UK law applies. Potential examples of such processing in a workplace context, which may be the subject such restriction, could include AI systems used in the recruitment or dismissal process or any performance related AI software used with respect to employee promotions or pay – provided that there is ***no*** meaningful human involvement in the process.

As noted above, this relatively strict GDPR regime is subject to exceptions which include, notably, where the solely automated processing is:

i. necessary for performance or entry into a contract between employer/employee;

ii. required or authorized by domestic law to which the employer is subject; or

iii. based on the employee's explicit consent.

Article 22(3) GDPR further protects employees by mandating that where employers do utilise AI systems to process personal data on the basis of the exceptions to the general prohibition in (i) and (iii) above, the employer must: (a) implement suitable measures to safeguard the employee's rights, freedoms and legitimate interests; (b) allow the individual the right to obtain human intervention on the part of the data controller; and (c) to express his or her point of view and to contest the decision. If "*special category*" personal data is concerned (e.g., data concerning health, racial or ethnic origin, or sexual orientation), decisions permitted on the grounds of (i) to (iii) above do not apply unless the employer relies on the Article 9 GDPR special condition for processing such data of either explicit consent (i.e., Article 9(2)(a) GDPR) or substantial public interest (i.e., Article 9(2)(g) GDPR). There may be certain challenges for using solely automated processing in an employment context. For example, obtaining explicit consent, satisfying the strict requirements for the same under the GDPR may be difficult to achieve in an employer-employee relationship given the imbalance of power present in such relationships. In addition, employees may withdraw any previously granted consent at any time. That said, provided there is "meaningful" human involvement in the decisions, Article 22 GDPR should not be implicated. Employers GDPR compliance obligations will therefore be more straightforward if AI is only being used to produce information that an employee then uses, perhaps alongside other information, to make decisions regarding other staff members.

DPIAs

The use of AI by an employer may require a DPIA, although this will ultimately depend on the particular use case. A DPIA is the process used to analyse, identify, and mitigate data protection risks that arise out of certain proposals or projects. A DPIA is necessary where a data controller is undertaking any type of processing that is likely to result in a high level of risk to the rights and freedoms of individuals. This may apply in an employment context where AI solutions are being used to make significant decisions about an individual's employment (e.g. hiring, pay and termination), engaging in workplace monitoring and/or where "*special category*" is being processed in support of the relevant services. AI-enabled systems also involve innovative technology, which is another factor pointing to the need to undertake a DPIA. DPIAs can be lengthy, time-consuming exercises. Where required, they also need to be finalized prior to the deployment of the AI software and should ideally be completed early in the process. Amongst other things, the DPIA will need to explain the relevant data flows through the AI system, identify the risks posed by the processing (e.g., potential biased outcomes, personal data breaches, opaqueness and unfair decisions), the employer's measures to mitigate those risks (e.g., due diligence, appropriate security measures, transparent notifications to data subjects and human oversight of decisions) and a balancing exercise between people's data protection interests and the competing interests of the business. It is also helpful to record in a DPIA how internal stakeholders were involved in the process and document the feedback received and how the processing had changed as a result. Despite the work involved, there is certainly value in the exercise in so far as properly assessing the data protection risks posed can lead to an employer asking the right questions of the third-party provider and mitigating legal risks posed by the adoption of the technology at the outset.

Access rights

The GDPR provides data subjects with several rights, including the right of access. This includes the right to receive copies of their personal data and other supplementary information. Individuals commonly exercise this right by issuing a data subject access request (**DSAR**). In general, employers' usual time scale to respond to a DSAR is "without delay" (and in any event within one month). Where employers utilise AI systems which process personal data which would fall under the scope of information required to be disclosed under a DSAR, this can be challenging given the difficulty in certain cases in explaining how technically advanced AI systems operate in practice and the potentially unintelligible way in which AI systems store data about individuals. It is therefore important that employers understand what data is being processed by the applicable system, how they can access this information in the event of a DSAR (and importantly, how it can be separated from other people's personal data) and how they can best respond to the request. This is particularly important where employers use AI systems created by third parties (as will often be the case) and it is recommended that employers consider how they might respond to DSARs in the future as part of their due diligence when engaging third parties for their AI services.

The EU AI Act

Introduction

The EU AI Act (**Act**) came into force on 1 August 2024. The Act represents the world's inaugural attempt at developing a legal framework to regulate AI. Whilst the Act recognises the importance of making use of AI and its many opportunities to drive efficiency and solve issues across myriad different sectors, it also recognises that AI systems creates risk which may need to be regulated to maintain trust in AI systems and avoid problematic uses of AI technology. The Act identifies four different risk levels which AI systems are placed into: (i) unacceptable risk; (ii) high-risk; (iii) limited risk; and (iv) minimal risk. Notably, certain uses in a workplace context may constitute unacceptable or "high-risk" activities under the Act.

We consider certain "high risk" scenarios under the Act below. The first scenario where this could apply concerns AI systems intended to be used for recruitment and in particular to place targeted job advertisements, analyse and filter job applications, and evaluate candidates. As the use of AI in recruitment continues to proliferate, employers must be mindful that they take into account their obligations under the Act. The second high-risk AI system relevant to employers is one intended to be used to make decisions affecting terms of work-related relationships. This could include making promotion or termination decisions, allocating tasks based on individual behaviour or personal traits or characteristics and monitoring and evaluating the performance of employees. Again, as more and more employers turn to AI to help in making key decisions regarding the makeup of their workforce, complying with the Act will be an important factor.

Providers vs. Deployers

The Act applies to different stakeholders across the AI ecosystem in different ways, including "providers", "deployers", "importers" and "distributors". A provider of AI systems is an entity which develops an AI system (or has one developed) which it then places on the market/puts the system into service under its own name or trademark. Conversely, a deployer is an entity that uses an AI system as part of its business. The distinction between a provider and deployer may not always be clear in practice. For example, a deployer may be treated as a provider where the deployer materially customizes or white labels a previously implemented AI system. Therefore, a company's legal and technology teams will need to closely collaborate around AI design and implementation to ascertain how the employer will be defined under the Act. The distinction is crucial as an organisation's obligations under the act depend on how it is classified.

Obligations on deployers of high-risk AI systems

Notwithstanding the considerations above, employers will typically be considered deployers of AI systems. Although providers of AI systems are subject to more onerous requirements than deployers, deployers remain subject to several compliance (and potentially costly) requirements. These include:

- taking appropriate technical and organisational measures to ensure the use of high-risk AI systems is in accordance with the provider's instructions for use;
- assigning human oversight who have the necessary competence, training and authority, as well as the necessary support;
- ensuring that input data is relevant and sufficiently representative in light of the intended purpose of the high-risk AI system, where the employer exercises control over the input data;
- monitoring the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, informing providers in accordance with the provider's post-market monitoring system;
- where the employer considers that the use of the high-risk AI system presents a risk to the health or safety, or to fundamental rights, of persons, informing without undue delay the provider or distributor and the relevant market surveillance authority, and suspend the use of the system;
- where a serious incident is identified, immediately informing the provider, and then subsequently the importer or distributor and the relevant market surveillance authorities;
- retaining logs automatically generated by the high-risk AI system to the extent such logs are under the employer's control for at least six months unless provided otherwise by applicable law; and
- informing workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system.

Extraterritorial effect

The Act is intended to have extraterritorial effect and applies to employers without a physical presence in the EU in certain circumstances. In respect of deployers that do not otherwise fall in scope because they are established or located within the EU, the Act will apply to the extent that the "output" of the AI system is "used in the EU." In other words, AI-generated predictions, content, recommendations, or decisions—if used in the EU—could potentially result in the application of the Act in perhaps unexpected circumstances. For example, the use of AI-generated outputs in the EU by a downstream deployer of an AI system from abroad may potentially trigger the application of the Act.

What penalties apply?

The consequences of failing to comply with the Act can be significant. For violations of banned AI applications, this can be up to the higher of €35 million or 7% of annual worldwide turnover. Fines of up to the higher of €15 million or 3% of annual worldwide turnover may apply for violations of the Act's obligations. Regarding the supply of incorrect information, fines of up to the higher of €7.5 million or 1.5% of annual worldwide turnover can be levied.

Conclusion

AI has the potential to transform the workplace as we currently know it. As discussed above, employers interested in harnessing the commercial benefits of AI-enabled tools must take care to consider the legal risks that the use of AI in the workplace will bring. In mitigating such legal risks, human oversight, transparency, adequate due diligence and an understanding of the technologies will be vital in the workplace. From a data protection perspective, employers' use of AI will likely involve the processing of personal data and therefore employers may need to consider obligations under the EU and UK GDPR. Compliance with the Act will also be crucial for many employers deploying AI systems, even those established outside of the EU given its extraterritorial effects.

Moreover, the use of AI by employers is likely to garner increasing legislative and regulatory scrutiny going forward. As already noted, the UK does not currently have specific legislation governing the use of AI systems and the Artificial Intelligence (Regulation) Bill proposed under the prior Conservative government will no longer progress. However, upon taking power in July, the new Labour government outlined the need for "*appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence models*". The government stopped short of promising to produce a new Bill and although it seems highly likely that further regulation is on the horizon, the form, detail and scope of the UK's regulation of AI remains to be seen. Employers should keep abreast of the likely forthcoming and increased regulation in this space in addition to their existing obligations. ■

MEALEY'S LITIGATION REPORT: ARTIFICIAL INTELLIGENCE
edited by Bryan Redding
The Report is produced monthly by

LexisNexis®

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: lexisnexis.com/mealeys
ISSN 2994-1105