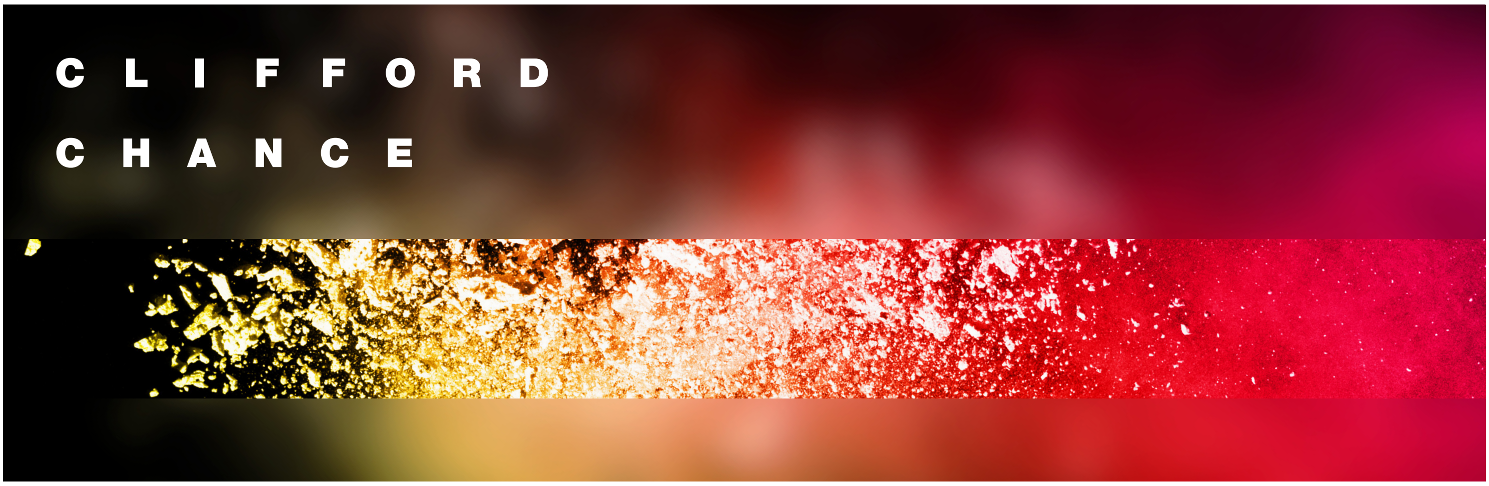


WHAT DOES THE EU AI ACT MEAN FOR EMPLOYERS?

The EU's Artificial Intelligence Act (EU AI Act)[1] will have a significant impact on employers and HR professionals who use, or plan to use, AI systems in their operations, recruitment, performance evaluation, talent management and workforce monitoring. The EU AI Act will not only affect organisations in the EU (and possibly EEA) Member States, it also has extra-territorial reach. In this briefing, we look at key considerations regarding the EU AI Act for employers and the practical steps businesses should take now.

What is the EU AI Act?

- The EU AI Act aims to ensure that AI in the EU or affecting the EU is trustworthy and human-centric and respects fundamental rights and values.
- The EU AI Act generally follows a risk-based approach. AI systems and models are classified, and requirements vary, depending on the potential impact of the AI system or model on human lives, fundamental rights and society.
- Several of the EU AI Act's rules specifically focus on AI in the workplace or AI in relation to employment and workers' management. Others, although not specific to the employment context, can also impact employers and HR professionals.
- Breach of the EU AI Act will give rise to fines with a maximum potential fine of the higher of EUR 35 million and 7% of the undertaking's global annual turnover for the most serious infringements.
- In most instances, it is for the EU Member States to lay down the rules on penalties and other enforcement measures, in line with the EU AI Act. National competent authorities will notably have powers to request information / documentation, to evaluate AI systems and to take necessary actions where there is an infringement.

[1] Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

Timeframe

The EU AI Act came into force on 1 August 2024. It will apply directly in EU Member States over a phased period.

2 February 2025	2 August 2025	2 August 2026[2]	2 August 2027
The prohibitions start applying (including as regards the use of AI to infer emotions in the workplace), as do the AI literacy requirements.	The requirements for providers of general-purpose AI (GPAI) models start applying, as do provisions around the EU AI Act's governance framework and Member State penalties.	The requirements for 'standalone' high-risk AI systems, including AI used in an employment context (e.g. for recruitment or decisions affecting work-related relationships), and the specific transparency obligations start applying, amongst other things.	The requirements for high-risk AI systems under specific sectoral legislation (e.g. re medical devices) start applying. This is also the date by which GPAI models placed on the market before 2 August 2025 need to comply with the EU AI Act.

The EU AI Act risk classification at a glance for employers

Key features of the EU AI Act include:

- **The prohibition of unacceptable risk AI practices.** Significantly for employers, this includes a ban on AI systems used to infer emotions in the workplace, subject to limited exceptions. Other examples include instances of AI systems deploying purposefully manipulative or deceptive techniques, exploiting certain vulnerabilities or categorising people based on biometric data to infer such things as race or trade union membership.

- **Strict obligations for AI systems classified as high-risk.** AI in the context of employment and workers' management is one of the areas that is considered high-risk under the EU AI Act. This includes AI systems intended to be used for (i) recruitment or selection purposes, or (ii) making decisions that affect terms of the work-related relationship, promotion or termination of work-related contractual relationships, allocating tasks on the basis of individual behaviour or personal traits or monitoring or evaluation of individuals in the workforce. Work-related contractual relationship is in principle a wider concept than a 'vanilla' employment relationship and could capture arrangements with platform workers, self-employed consultants and staff supplied via employment agencies. The EU AI Act lays down substantial obligations for high-risk AI systems, with additional requirements as regards the deployment of high-risk AI systems in the workplace.

- **Specific transparency obligations for certain AI systems or uses** to inform users about their nature, purpose or operation, or to ensure they are aware that content is artificially generated or manipulated. There are for example specific transparency requirements regarding AI systems that directly interact with people such as chatbots, emotion recognition and biometric categorisation systems, as well as generative AI systems. These requirements can apply on top of the requirements for high-risk AI systems.

[2] This is the date on which the EU AI Act's requirements start to apply by default.

- **Rules to regulate GPAI models**, with requirements for all GPAI models and additional requirements for those with systemic risk.
- **General AI literacy requirements.** Providers and deployers of AI systems are required to ensure a sufficient level of AI literacy among their staff and other persons dealing with the operation and use of AI systems on their behalf.

A focus on high-risk AI systems – what employers need to know

Substantial requirements

In addition to the EU AI Act significant risk and quality management system requirements, high-risk AI systems are also subject to other substantial obligations that aim to ensure their trustworthiness and mitigate the risks. These include:

- **Data quality**: The data used to train, validate or test a high-risk AI system must be relevant, sufficiently representative, free of errors 'to the best extent possible', and scrutinised for possible biases that are likely to affect health and safety or lead to discrimination. Where it is the deployer (e.g. the employer) that has control over the input data, it must ensure that such data is relevant and sufficiently representative taking account of the system's intended purpose. In addition to the EU AI Act obligations, operators must of course respect data protection rules.
- **Technical documentation**: The provider must prepare and maintain detailed technical documentation that describes the system's general characteristics, intended purpose, performance including capabilities and limitations in performance and instructions for use for the deployer, as well as the system's design specifications and the data and methods used to develop and test it.
- **Conformity assessment**: The provider must ensure that the AI system undergoes a self-assessment or a third-party assessment, as applicable, to verify that the system complies with the requirements of the EU AI Act for high-risk AI systems and issue an EU declaration of conformity. In principle, the self-assessment procedure based on internal control will apply to employment and workers' management AI tools classified as high-risk.
- **Human oversight**: High-risk AI systems must be designed and developed to allow for effective human supervision. Different types of oversight measures are envisaged in the EU AI Act: (i) those that are built into the AI system by the provider, and (ii) those that are identified by the provider before the AI system is placed on the market or put into service and that are appropriate to be implemented by the deployer. The high-risk AI system must be provided to the deployer in such a way that the people to whom human oversight is assigned can, amongst other things, properly understand its capacities and limitations, monitor its operation, interpret its output, decide not to use it, disregard its output and safely halt it e.g. through a stop button. The deployer must assign human oversight to people having the necessary skills – including an adequate level of AI literacy – authority and support.

- **Transparency and instructions for use**: By design, high-risk AI systems must be sufficiently transparent, including through their operation to enable deployers to interpret their output and use them appropriately. The provider must also provide meaningful information about the system's characteristics, capabilities, expected performance and limitations including via the instructions for use that must accompany the system. The deployer must take the necessary measures to ensure it uses the system in accordance with those instructions for use.
- **Deployer's specific information obligations**: Deployers of 'standalone' high-risk AI systems that make or assist in making decisions related to natural persons must inform them that they are subject to the use of the system. In the field of employment and HR, deployers who are employers must, before using a high-risk AI system in the workplace, inform workers' representatives and the affected workers that they will be subject to the use of the system. Where applicable, this information should be provided in accordance with EU and national rules, procedures and related practices on the provision of information to workers and their representatives. These transparency requirements are in addition to the transparency obligations referred to above, that are not limited to high-risk AI systems.
- **Accuracy, robustness and cybersecurity**: The provider of a high-risk AI system must ensure that the system achieves an appropriate level of accuracy, robustness and cybersecurity, and that it is as resilient as possible with respect to errors, inconsistencies or malicious attacks.
- **Record-keeping**: The provider and the deployer of a high-risk AI system each have responsibilities in terms of keeping records of the system's functioning, performance and use, and making them available to the competent authorities upon request.
- **Monitoring and reporting**: Whilst their obligations vary, both the provider and the deployer of a high-risk AI system must monitor and report incidents, malfunctions or risks that may affect the system's compliance or performance and they must co-operate with the competent authorities in case of investigations or audits.
- **Individual decision-making information obligations**: In certain circumstances, and on request, deployers must provide an explanation to affected persons with respect to individual decision-making on the basis of the output from a 'standalone' high-risk AI system.
- **Human dignity, non-discrimination and fundamental rights**: A consistent underlying aim of many of the EU AI Act provisions is that AI should not amplify existing discrimination or become a source of discrimination.

High-risk but not high-risk?

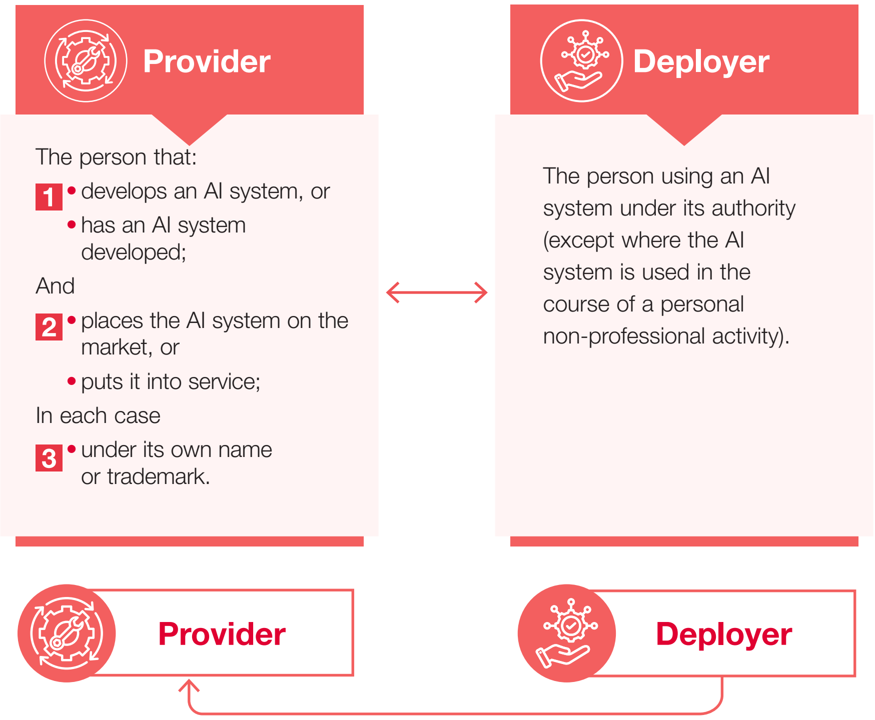
Where an AI system comes within one of the listed high-risk use cases, there might still be exceptional circumstances where it isn't considered to pose a significant risk of harm and hence shouldn't be deemed high-risk, e.g. because it doesn't materially influence the outcome of decision-making. Examples include situations where the AI system is only intended to perform a narrow procedural task (e.g. it simply classifies incoming documents into categories), to improve the result of a previously completed human activity, or to perform a task that is only preparatory to an assessment relevant for the purposes of the use case in question (e.g. smart solutions for file handling, or AI systems used to translate initial documents). If the relevant system performs profiling, however, this derogation will not apply and the AI system will be classified as high-risk.

In order to make use of the derogation, the provider must conduct a documented self-assessment and register in an EU database, in each case prior to placing on the market or putting into service the AI system. If a provider uses the self-assessment derogation procedure to circumvent the EU AI Act, it exposes itself to substantial fines.

Careful consideration by the provider is essential before seeking to rely on this derogation and in particular in the employment context. To assist, the European Commission is expected to provide guidelines by no later than 2 February 2026, together with a comprehensive list of practical examples of use cases of AI systems that are high-risk and use cases that are not.

The critical question of the employer's role: Provider or deployer?
Different rules apply to different operators in the AI value chain (providers, deployers, importers, distributors, etc.), with the provider bearing the brunt of the obligations under the EU AI Act. That said, and as this briefing illustrates, deployers are also subject to significant requirements, in relation to high-risk AI and beyond.

Ascertaining whether the employer is a deployer or can be considered a provider is crucial.



Provider

The person that:

1
- develops an AI system, or
- has an AI system developed;

And

2
- places the AI system on the market, or
- puts it into service;

In each case

3
- under its own name or trademark.

Deployer

The person using an AI system under its authority (except where the AI system is used in the course of a personal non-professional activity).

An employer that is a deployer can be deemed a 'provider' in relation to a high-risk AI system where:

- It puts its name or trademark on a high-risk AI system already placed on the market or put into service.
- It makes a substantial modification to a high-risk AI system already placed on the market or put into service and it remains high-risk.
- It modifies the intended purpose of an AI system, including a GPAI system, in such a way that it becomes high-risk.

What is the impact on multinational employers?

The EU AI Act doesn't only apply to businesses that use AI systems in the EU. One of the circumstances in which the EU AI Act can apply to multinationals is if their AI systems outside the EU are used to make decisions in relation to the workforce based in the EU. For example, an employer based in the US using an AI tool to measure employee performance globally, including employees based in the EU, to allocate bonuses could be caught by the EU AI Act's provisions. In addition, the deployment of group-wide global recruitment systems, including applicants based in the EU, will need to meet the standards of the EU AI Act.

The EU AI Act also applies to third-country providers of AI systems that are placed on the market or put into service in the EU (likewise as regards third-country providers of GPAI models placed on the EU market); this could catch multinational employers who are treated as providers in certain cases. This extra-territorial reach should, in addition, inform an employer's approach to the procurement of AI technologies for the workplace; addressing what needs to be included in vendor management agreements in terms of, for example, transparency, information provision and co-operation obligations so that both parties can address and meet their legal obligations under the EU AI Act and any other applicable legislation.

Additional legal considerations

In addition to the specific requirements of the EU AI Act, other legal obligations should be considered, in particular any applicable data protection requirements as well as employment law considerations, including workforce consultation obligations, laws on discrimination as well as liability issues in relation to AI.

Data protection: The EU General Data Protection Regulation (EU GDPR) will apply if an AI tool processes employee personal data as part of the activities of an employer establishment in the EU / EEA, or in order to monitor the behaviour of EU-based employees, for example where tools analyse employees' emails and/or instant messaging to assess work rates or quality of communications. The EU GDPR imposes a wide range of obligations, generally familiar to European employers, designed to ensure (very broadly speaking) the fair and proportionate processing of employee personal data and to allow employees to exercise a degree of control over their data.

Particularly relevant to the processing of employee data by AI tools are the EU GDPR's tight restrictions – amounting to a complete prohibition in some circumstances – on the use of automated systems to make significant decisions about employees or other individuals without human intervention. There may also be additional requirements around the lawful basis when processing employee data in certain Member States such as in Germany.

Employee representative consultation: Depending on the jurisdiction within the EU, there may be independent requirements to consult with employee representatives, trade union or domestic or European works councils before using AI tools. These are typically required in the Netherlands, Germany, Luxembourg, France and Italy.

EU AI Act: Guidance needed

Guidance is planned and expected on numerous important questions under the EU AI Act, including to support its practical implementation.

For instance, guidelines are expected in relation to the prohibitions, before they enter into force on 2 February 2025. This may be of direct relevance to employers as several prohibitions could impact them, starting with the ban on systems to infer emotions in the workplace. Other relevant examples concern guidelines on the application of requirements for high-risk AI and related responsibilities along the AI value chain, as well as those on transparency.

Beyond guidance, voluntary initiatives and pledges?

To bridge the gap until the EU AI Act starts to apply, there is an EU initiative known as the AI Pact. It aims to foster early implementation by businesses of the EU AI Act, encouraging the sharing of processes and best practices as well as voluntary pledges to anticipate some of the EU AI Act's requirements.

The EU AI Office recently released draft pledges, focusing on aspects that reflect some of the EU AI Act's requirements for high-risk AI and transparency. That said, certain pledges are broader and not necessarily tied to a given type of AI system or use. For deployers, potential voluntary commitments under the draft pledges include:

- Providing explanations to people when a decision about them is prepared, recommended or taken by AI.
- Informing affected workers and workers' representatives when deploying AI at the workplace.
- Ensuring people are informed when directly interacting with an AI system.

The pledges will be discussed during a workshop in September, with the target of collecting official signatures from businesses on final pledges in the Autumn.

In addition, in some jurisdictions, individual employee consultation / notification may also be required prior to implementing AI monitoring tools. Such notification requirements may apply in addition to the transparency requirements under the EU AI Act and data protection legislation.

Individual and collective consultation will in many cases also be required where the use of AI tools will result in redundancies and/or changes in the nature of the work undertaken.

Discrimination laws: Measures should be implemented to ensure that discrimination laws are not infringed as a result of the way in which an AI tool's output is used (for example, in the context of assessing who should be recruited or promoted). If the tool's output results in a less favourable impact / outcome for particular groups with 'protected characteristics' for the purposes of applicable anti-discrimination legislation, this could give rise to discrimination claims.

If AI tools are used to monitor attendance or productivity (for example, frequency of 'comfort breaks'), consideration needs to be given to whether this could provide the platform for discrimination claims by employees with health conditions that necessitate more frequent breaks.

The proposed manner in which an AI tool is to be deployed should also be assessed to ascertain whether it could result in indirect discrimination as a consequence of its application putting specific 'protected groups' at a particular disadvantage. If such an audit indicates 'particular disadvantage', an indirect discrimination claim can still be defended if a legitimate aim is identified for the use of the AI tool and the tool is a proportionate means of achieving that aim. Consideration should be given to whether the process should also identify relevant legitimate interests and whether there are other, less discriminatory, means of achieving the same objective.

Health and safety: In some circumstances the use of AI technology may have a significant adverse impact on the mental health of staff who are psychologically impacted by a sense of constant monitoring and inability to maintain a work-life balance in breach of an employer's legal obligations to maintain a safe place of work. This may particularly be the case where AI tools are used for any form of monitoring purpose; for example, work rate, attendance levels, stress levels. In addition, where AI tools and the information they generate are not reliable (AI hallucinations), this too could result in unsafe working conditions.

Scope creep: Care will need to be taken to prevent scope creep, i.e. where the original purpose of deploying the AI tool evolves and data that was collected for one purpose, such as training requirements, is later used for other purposes; for example, disciplinary purposes. Scope creep could result in unlawful data processing and, potentially, breach of other legal obligations, including if the workforce was not informed of and/or consulted about such additional processing.

Liability: AI raises important questions of liability, which need to be considered in the light of existing rules as well as upcoming and developing rules such as the revised Product Liability Directive and the proposed AI Liability Directive.

A move towards dedicated EU legislation on AI in the workplace?

There have been suggestions that specific EU-level legislation regulating the use of AI in the workplace is being considered. This is something that employers should monitor closely.

Different jurisdictions are taking different approaches

Non-EU jurisdictions in which an employer operates may have adopted a different (and possibly conflicting) approach to AI management, or may do so in the future, and employers will have to adopt an appropriate strategy to navigate this. To add to the complexity, some EU Member States may also have other AI related laws and initiatives that will also have to be factored into working practices by employers. Whilst the EU AI Act seeks to harmonise rules on AI in the EU, on the specific issue of worker protection, it does not prevent legislation or administrative provisions that are more favourable to workers in terms of protecting their rights as regards the use of AI systems by employers, or the application of collective agreements which are more favourable to workers.

United Kingdom

The EU AI Act will not take effect in UK law, although it will have some effect in the UK by virtue of its extra-territoriality.

There is, as yet, no specific UK legislative regime addressing AI, either in the workplace or otherwise. The new UK government proposes to introduce 'appropriate legislation to place requirements on those working to develop the most powerful' AI models and has stated (on 26 July) that it proposes to consult on this shortly, over a two-month period. It is widely believed that the Bill will focus primarily on ChatGPT-style foundation models.

Prior to the election, the Labour party manifesto document: **Plan to Make Work Pay** stated that if elected a Labour Government would: '… work with workers and their trade unions, employers and experts to examine what AI and new technologies mean for work, jobs and skills, and how to promote best practice in safeguarding against the invasion of privacy through surveillance technology, spyware and discriminatory algorithmic decision making. At a minimum Labour will ensure that proposals to introduce surveillance technologies would be subject to consultation and negotiation, with a view to agreement of trade unions or elected staff representatives where there is no trade union'. Whether these proposals will feature in the draft Employment Rights Bill that is expected within the first 100 days of Government (i.e by 12 October 2024) remains to be seen.

The Information Commissioner's Office (ICO) updated its **Guidance on artificial intelligence and data protection** in March 2023, spelling out implications of the UK GDPR for AI systems involving the processing of employee (or other) personal data. It acknowledged that there will be a need for future review and updating to take account of technological development, with a specific plan to consult and update in spring 2025. The **Health and Safety Executive** and the **Equality and Human Rights Commission** (EHRC) both responded with high-level statements about their approach to the regulation of AI, but these do not amount to detailed guidance on the application of existing law to AI systems. The Department for Science, Innovation and Technology, with input from the ICO, the EHRC and others, has published more specific **Guidance** on procuring and deploying AI responsibly in the HR and recruitment sector.

United States

In the United States, there is no single overarching legislation that addresses AI in the workplace. Employers' use of AI tools is subject to federal laws that prohibit employment discrimination, federal AI-focused legislation and guidance, and state and local employment and AI-focused laws. These various efforts address, among other considerations, algorithmic discrimination, automated employment decision-making, and concerns at the intersection of privacy and employment.

Federal Laws That Prohibit Employment Discrimination: US federal laws prohibit employment discrimination based on race, colour, ethnicity, sex, age, national origin, religion, disability, pregnancy, military services and genetic information. An employer must ensure compliance with a range of anti-discrimination laws. The Equal Employment Opportunity Commission (EEOC) enforces these laws and is authorised to investigate discrimination charges and to bring lawsuits. Its guidance does not have the force of law, but courts may look to it when rendering judgments.

The EEOC has, among other things, produced **Guidance** highlighting concerns at the intersection of the Americans with Disabilities Act (ADA) and AI, such as biased results, problems with accessibility for visually or auditorily impaired candidates, and the need for reasonable accommodation, and **Guidance** addressing the use of AI in the employee selection process. The EEOC has also been involved in AI discrimination lawsuits, some of which are ongoing. These lawsuits help shape regulation on the use of AI in the workplace.

Federal Government AI-Focused Legislation and Guidance: The US federal government has increasingly focused on the development, design and use of AI in employment, including via, for example, the AI Training Act requiring, among other things, that the U.S. Office of Management and Budget Director establishes an AI training program for the acquisition workforce.

Other legislation has been introduced in Congress, including **The No Robot Bosses Act**, which aims to ban reliance on automated decision systems in employment, and requires pre-deployment testing for discrimination and biases, and human oversight of output and **The Stop Spying Bosses Act**, which would require employers to disclose workplace surveillance activities, prohibit collection of sensitive employee data and create guidelines for automated system use.

In addition, in April 2024, in response to President Biden's **Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**, the U.S. Department of Labor issued "**Artificial Intelligence and Worker Well-being: Principles and Best Practices for Developers and Employers**". Also in April 2024, the U.S. Labor Department's Wage and Hour Division issued a **Field Assistance Bulletin** to provide guidance on the applicability of the Fair Labor Standards Act and other federal labor standards to employers' increasing use of AI. The U.S. Labor Department's Office of Federal Contract Compliance Programs issued **Guidance** on federal contractors' use of AI in employment decisions. Although these guidelines apply to federal contractors, they can be instructive for other employers.

State and Local Laws: US states and local governments continue to pursue and enact AI-focused and other related legislation. Initiatives of note include **Colorado's Concerning Consumer Protections in Interactions with Artificial Intelligence Systems Act**, enacted on 17 May 2024, governing developers and deployers of AI systems affecting consumers, Illinois' **Artificial Intelligence Video Interview Act**, effective 1 January 2020, mandating notification and other requirements when an employer asks applicants to record video interviews and uses AI analysis of such videos, and New York City's **law** on automated employment decision tools, which took effect on 5 July 2023, mandating bias audits for AI tools used in employment decisions.

Action points for employers

The EU AI Act will introduce a comprehensive and complex regulatory framework for AI that will have a significant impact on employers and HR professionals who use or plan to use AI systems in their operations. In preparation for the new regime, employers should:

- Audit their current and proposed use of AI systems in the employment / HR context.
- Determine whether any of the AI tools are used, or are likely to be used, to make decisions in relation to the workforce based in the EU.
- Analyse whether any existing or planned uses could be caught by the prohibitions, and take necessary steps to modify or end any such use prior to 2 February 2025 when the prohibitions start to apply.
- Assess whether any of the AI tools would be regarded as 'high-risk' for the purposes of the EU AI Act, or if not, identify what their status under the EU AI Act is and any related requirements.
- Confirm their role in the AI value chain and the corresponding obligations; this should also address the risk of being classified as a provider.
- Consider what principles, policies and procedures should be implemented to ensure that the AI tools are developed, deployed and used in accordance with the EU AI Act's requirements and other applicable requirements.
- Assess what safeguards and controls are, or should be, in place to prevent or address any issues or incidents.
- Consider what internal mechanisms should be put in place to facilitate the reporting of AI system malfunctions.
- Consider what training and guidance should be provided to the staff who are involved in the development or deployment of their AI tools to ensure, amongst other things, that they are aware of their roles and responsibilities, of the risks and possible harm, and of the rights and expectations of the workforce and other stakeholders.

- Implement awareness raising, training and guidance for top management, including as regards the risks and opportunities for the organisation and their responsibilities.
- When planning to use an AI system in the workplace, identify what information needs to be provided to the affected workers and workers' representatives and ensure they are duly informed, in accordance with applicable requirements including the EU AI Act and any applicable EU or national rules, procedures and related practices on information of workers and their representatives.
- More generally, identify what consultation and communication is required in relation to domestic or European Works Councils, trade unions and individual employees who are or will be affected by, or subject to, the AI tools.
- Decide how staff will be provided with information about relevant AI tools, as well as their rights and how to seek explanations or redress.
- Consider what information needs to be provided to candidates who may be exposed to AI tools in the context of the recruitment process, and how to provide that information.
- Consider what approach to adopt to the life cycle management of AI within the company and the component parts of a multidisciplinary approach to it: legal, HR, workforce, IT, procurement all being obvious candidates.
- Assess and incorporate the employment / HR aspects within the organisation's broader AI strategy, governance and risk management framework, and leverage, and co-ordinate with, existing mechanisms.
- Consider what procedures should be put in place to review and update the AI tools regularly to ensure that they remain compliant, accurate, robust and secure, and that they reflect the changing needs and expectations of the organisation, the employees and other stakeholders.
- Keep a watching brief for the publication of further legislation and relevant guidance under the EU AI Act and adapt accordingly.
- Consider the existing and evolving global regulatory and compliance landscape, on AI-focused legislation, as well as applicable employment, discrimination, health and safety, privacy and other relevant laws and codes of practice impacting the use of AI tools in an employment context and also in a wider workforce context. For example, the proposed EU Directive aimed at improving conditions in platform work.

CONTACTS

Alistair Woodland
Head of UK Employment and Co-head of Global Employment
London
T: +44 207006 8936
E: alistair.woodland@cliffordchance.com

Floris van de Bult
Co-head of Global Employment
Amsterdam
T: +31 20 711 9158
E: floris.vandebult@cliffordchance.com

Ines Keitel
Partner
Frankfurt
T: +49 69 7199 1250
E: ines.keitel@cliffordchance.com

Dessislava Savova
Partner, Head of Continental Europe Tech Group
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Holger Lutz
Partner
Frankfurt
T: +49 69 7199 1670
E: holger.lutz@cliffordchance.com

AUTHORS

Tania Stevenson
Knowledge Director
London
T: +44 207006 8938
E: tania.stevenson@cliffordchance.com

Alexander Kennedy
Knowledge Director – CE Tech Group
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Inna Jackson
Tech Knowledge & Innovation Attorney – Americas
New York
T: +1 212 878 3292
E: inna.jackson@cliffordchance.com

For more detailed information and insights on the EU AI Act, you can also refer to our publications **here**.

For a high level overview please see our briefing: **Understanding the EU AI Act: implications for employers.**

CLIFFORD

CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word ‘partner’ to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.