AI in the workplace: the changing regulatory landscape

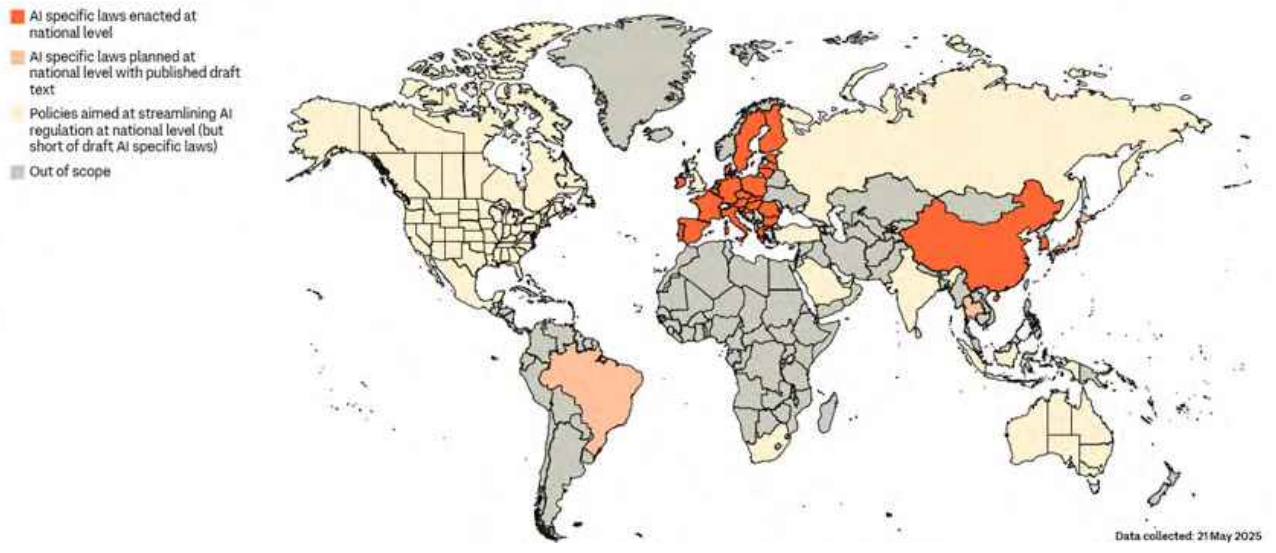
This briefing explores the changing AI regulatory landscape, with a particular focus on the European Union, the UK, the US, China, Japan, Singapore and India.

I. Introduction

The use of artificial intelligence (***AI***) has grown in recent years. In an employment context, AI is quickly becoming a valuable tool for recruitment, work allocation, employee monitoring and many other aspects of the working relationship.

However, when AI is improperly trained or used various risks may arise, for which employers should be cautious. For example:

- **Discrimination**: certain uses of AI may lead to discrimination against certain groups of workers based on their protected characteristics. AI systems used for recruitment, performance management or other decision-making processes may be based on data that is biased, incomplete or outdated and may therefore produce outcomes that are unfair, inaccurate or inconsistent.
- **Impact on diversity**: the use of AI-powered HR tools for recruitment, performance evaluation, promotion or dismissal could have a negative impact on diversity if the AI system relies on biased data and makes decisions about the workforce on that basis.
- **Collective obligations**: employers should consider any applicable collective obligations when rolling out AI in the workplace and establish a regular and structured dialogue with employee representatives on the progress of AI implementation.
- **Data privacy**: employers train their AI and people correctly, before inputting personal data into AI-powered applications, and ensure compliance with data privacy laws and other AI specific laws.
- **Employee activism and/or unrest**: there is potential for employee activism and/or unrest if the implementation of AI in the workplace is mishandled, or in response to fears around AI generally.



As demonstrated on the heat map[1] above, there is consensus that the benefits of AI can only be realized if there is appropriate regulation. In March 2024, the United Nations (the ***UN***) General Assembly adopted a resolution co-sponsored by more than 120 UN Member States which suggests 'develop[ing] and support[ing] regulatory and governance approaches and frameworks related to safe, secure and trustworthy artificial intelligence systems'.[2]

More recently, on 5 September 2024, countries including the UK, US, and the European Union (the ***EU***) signed the Council of Europe's Framework Convention on AI (the ***Framework Convention***).[3] The Framework Convention is the first legally binding international treaty in relation to AI. It commits parties to collective action to protect the public from potential misuse of AI.

AI developers also recognise the value that regulation can bring through increasing safety and trust in the systems they build and, in some cases, have made voluntary commitments. In May 2024, on the opening day of the AI Seoul Summit, 16 leading AI tech companies made voluntary AI safety commitments.[4] Further details of these commitments can be found in our blog post here.

However, the approach to regulation has been varied to date. In the EU, the Artificial Intelligence Act (the ***AI Act***) envisages a risk-based approach to regulating AI systems, from limited to prohibited AI systems/use cases and general-purpose AI models. Other countries, such as the UK and Japan, have adopted a lighter touch approach based on principles and guidance to encourage innovation.

II. The EU: the AI Act

On 13 March 2024, the European Parliament adopted the final version of the AI Act.[5] The AI Act is regarded as the world's first attempt to comprehensively regulate the use of AI. It aims to promote the development of 'trustworthy' AI and to ensure a high level of protection against the potential harmful effects of AI systems.

The AI Act follows a risk-based approach based on the potential impact of AI systems. Accordingly, AI systems will be categorised into the following risk categories in the future:

- AI systems with unacceptable risk;
- AI systems with high risk;
- AI systems with special transparency obligations; and
- AI systems with minimal risk.

In principle, the higher the risk, the stricter the obligations imposed on the providers[6] and deployers[7] of such systems.

1. Prohibited under the AI Act: AI systems with unacceptable risk

Article 5 of the AI Act provides that 'AI systems with unacceptable risk' (defined as systems that are suspected of violating fundamental rights enshrined in the Charter of the European Union) are **completely banned** from 2 February 2025.

In an employment context, this category includes **systems designed to infer the emotions of natural persons in the workplace and systems that categorise natural persons individually based on their biometric data**, unless they are to be installed or placed on the market for medical or safety reasons.

2. AI systems with high risk

The 'high-risk' category will include AI systems that could potentially have a **detrimental impact on the health, safety and fundamental rights of data subjects**.

In an employment context, this will include the following AI systems:

- AI systems intended to be used for the **recruitment or selection of natural persons**, in particular to place targeted job advertisements, analyse and filter job applications and evaluate candidates; and
- AI systems intended to be used to **make decisions affecting terms of work-related relationships**, the **promotion** or **terminations** of work-related contractual relationships, to **allocate tasks** based on individual behaviour or

---

1 AI specific laws – current and pending regulation in selected jurisdictions. Data collected: 21 October 2024.

2 UN: 'Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development'. https://news.un.org/en/story/2024/03/1147831

3 'Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law'. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225

4 Frontier AI Safety Summits, May 2024. https://www.gov.uk/government/publications/frontier-ai-safety-commitments-ai-seoul-summit-2024/frontier-ai-safety-commitments-ai-seoul-summit-2024

5 Artificial Intelligence Act. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

6 A *provider* under Article 3(3) of the AI Act, is a natural or legal person or body that: (i) develops an AI system or general-purpose AI model or has an AI system or general-purpose AI model developed; and (ii) places that system or model on the market, or puts that system into service, under the provider's own name or trademark, whether for payment or free for charge.

7 A *deployer* under Article 3(4) of the AI Act, is a natural or legal person or body using an AI system under its authority, except in the course of a personal non-professional activity.

personal traits or characteristics or to **monitor and evaluate the performance and behaviour** of persons in such work-related relationships.

However, Article 6(3) of the AI Act provides an exception for high-risk systems that do not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making in relation to **subordinate support activities**.

The use of high-risk AI systems will be **permitted in principle**. However, it will be subject to **additional obligations**, depending on whether employers are categorised as 'providers' or 'deployers'.

3. Obligations as a deployer

Employers will generally qualify as deployers if they merely **purchase and use existing and externally pre-trained AI systems**.

It is unclear whether employers will become deployers if they simply allow their employees to use freely accessible AI systems via the internet or tolerate their use.

Under Article 26, deployers of high-risk AI systems will be subject in particular to the following obligations:

- Employers must only use high-risk AI systems **in accordance with the instructions for use** shared by the provider and the systems must be **constantly monitored**. If there is reason to believe that the use of the system may present a risk to health, safety or fundamental rights, the use of that system shall, without undue delay, be suspended and comprehensive reporting obligations must be fulfilled. Similar reporting obligations apply if the use of the AI system results in a 'serious incident' (as defined in Article 3(49)).
- To the extent the employer exercises control over the input data, they must ensure that **input data is relevant and sufficiently representative in view** of the intended purpose of the high-risk AI system.
- Employers must **assign human oversight** for high-risk AI systems to individuals with the necessary competence, training, authority and support. This will likely require employers to provide training to such individuals.
- Employers must **keep the logs** automatically generated by the high-risk AI system for at least six months.
- Employers may have to **inform the affected employees and employee representatives** before putting into service or use a high-risk AI system.
- If a high-risk AI system makes decisions about natural persons or assists in such decisions, **employers shall inform such natural persons that they are subject to the use of the high-risk AI system**.
- Employers must use the information provided to them by the provider as part of the **data protection impact assessment** they are required to perform.

4. Obligations as a provider

Employers which do not develop AI systems or place them into the market may exceptionally be classified as providers if they make a **substantial modification** to an existing high-risk AI system in such a way that it remains a high-risk AI system, or if they **modify the intended use of an AI system** in such a way that it becomes a high-risk AI system.

Employers which are classed as a 'provider' must fulfil the additional provider obligations under Article 16 of the AI Act. This includes ensuring that the high-risk AI system fulfils the general requirements for trustworthy AI in terms of data governance, technical documentation and record-keeping, transparency, human oversight, accuracy, cybersecurity and robustness. They must also undergo a conformity assessment procedure and introduce a quality management system. They are also subject to strict registration, documentation and information obligations.

5. Other obligations

The AI Act also sets out other obligations that employers must observe when using any AI systems. For example, under Article 4, employers will be required to take measures to ensure their staff and other persons dealing with the operation and use of AI systems on their behalf have a sufficient level of AI literacy.

6. Sanctions

Member States must set effective, proportionate and dissuasive penalties, including fines, for breaches of the requirements of the AI Act.

The AI Act sets out the following **thresholds for the determination of fines**:

- The use of a prohibited AI system can result for any person in fines of up to €35m or up to seven per cent of the previous year's global turnover, whichever is higher.
- The breach of obligations by an operator (ie an importer, deployer (employers will predominantly fall under this category), provider, product manufacturer, authorised representative or distributor) of high-risk AI systems can result in, among other things, fines of up to €15m or up to three per cent of the previous year's global turnover, whichever is higher.

The AI Act will provide natural or legal persons with the right to **lodge a complaint** if they have grounds to consider that there has been an infringement of the AI Act. This right may be used by employees in connection with labour law disputes in the future.

7. When will the AI Act apply?

Article 113 of the AI Act provides for a transitional period, meaning that the AI Act will be **generally applicable 24 months** after its entry into force, ie from 2 August 2026.

However, a few individual provisions will be applicable earlier or later. In particular, as already mentioned above, AI systems with unacceptable risk are prohibited as of 2 February 2025 **(six months** after the AI Act came into force). The aforementioned AI literacy obligation entered in to force on the same date.

8. Outlook

The AI Act was formally published in the Official Journal of the EU on 12 July 2024, and it officially came into force on 1 August 2024 (20 days after publication). Once it took effect, the AI Act became **directly applicable law in the Member States**, meaning that no further implementation by the Member States was required.

The AI Act is expected to have a significant impact on the use of AI systems by companies and organisations. The impact will extend beyond the EU as the AI Act will apply to foreign companies which provide, import, distribute or manufacture AI systems in the EU market. In an employment context, it will shape the use of AI in recruitment, decision-making and disciplinary actions, amongst others, and it may set the tone for future regulation in other jurisdictions.

III. UK

Despite positioning itself as a champion of AI safety, as the host of the first international AI Safety Summit in November 2023, the **UK has adopted a pro-innovation approach to AI regulation to date and the government is yet to enact any AI specific legislation.**

In March 2023, the UK government published a **white paper on AI regulation** which established a regulatory framework for AI under which existing regulators would **monitor** the use of AI in their sectors by applying existing laws (the ***White Paper***).[8] In doing so, regulators are required to interpret and apply five cross-sectoral principles (the ***Principles***):

- **Safety**, security and robustness;
- Appropriate **transparency** and explainability;
- **Fairness**;
- **Accountability** and **governance**; and
- **Contestability** and **redress**.

The White Paper states that the Principles will be issued on a non-statutory basis initially and that, following an initial period and once parliamentary time allows, the government would, subject to monitoring, '**strengthen and clarify regulators' mandates**' by introducing a **statutory duty** to have due regard to the Principles.

On 6 February 2024, the UK government published its response to the consultation on the White Paper (the ***Response***), in which it confirmed that the **non-statutory approach would continue**.[9] The Response also noted a number of steps to support the regulatory framework, such as the development of a central function to boost regulators' AI capabilities and the recruitment of a multidisciplinary team to carry out cross-sectoral risk monitoring within the Department for Science, Innovation and Technology (the ***DSIT***).

In April 2024, the UK government also launched the **AI and Digital Hub** (the ***Hub***), a government-funded scheme to help AI developers access informal advice from regulators on how to develop and release AI models. The Hub was introduced as a 12-month pilot scheme and a final decision will be taken on its future in 2025.

1. Employment-specific risks and regulation

As stated in the Response, the UK government's position is that the 'robust system of legislation and enforcement for employment protections […] sets a strong foundation for workers'. Nevertheless, some steps have been taken to address employment-specific risks:

- In March 2024, the government published **guidance on responsible AI in recruitment**, which identifies the possible risks of using AI in recruitment and hiring processes and sets out a range of considerations for organisations.[10]
- The DSIT is **working** with the Equality and Human Rights Commission (the ***EHRC***) and the ICO to

[8] 'A pro-innovation approach to AI regulation' (29 March 2023). https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

[9] DSIT, 'Consultation outcome: A pro-innovation approach to AI regulation: government response' (6 February 2024). https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response

[10] Guidance: 'Responsible AI in Recruitment' (25 March 2024). https://www.gov.uk/government/publications/responsible-ai-in-recruitment-guide/responsible-ai-in-recruitment

develop solutions to address bias and discrimination in AI, including recruitment and decision-making.

However, there have been calls for further steps to be taken. For example, the Trades Union Congress (the ***TUC***) has argued that 'urgent action is needed to ensure that people are protected from the risks and harms of AI-powered decision making in the workplace'.

In April 2024, the TUC published a draft bill, the **Artificial Intelligence (Regulation and Employment Rights) Bill** (the ***TUC Bill***), and an accompanying paper.[11] The TUC Bill proposes various rights and protections, including a legal duty on employers to consult trade unions on the use of high risk and intrusive forms of AI in the workplace and to impose protections against unfair dismissal by AI.

2. Potential legislation

In the Response, the then government acknowledged the potential for 'more targeted, binding requirements on developers of highly capable general-purpose AI models in the future'. However, it emphasised that, due to the speed with which AI is developing, it would **take the time to understand the risks and appropriate mitigations before imposing regulations.** Furthermore, the government stated that it would only legislate if 'existing mitigations were no longer adequate', it was 'not sufficiently confident that voluntary measures would be implemented effectively' and it was confident that it could 'significantly mitigate risk without unduly dampening innovation and competition' via legislation.

In July 2024, voters elected the Labour Party to form a **new government**. The Labour Party's stated position on AI regulation during the election was broadly the same as the former government, but it remains to be seen what approach will ultimately be taken.

In its election manifesto,[12] the Labour Party committed to supporting the development of the AI industry, whilst also taking regulatory steps. It promised to 'create a new Regulatory Innovation Office' and to 'ensure the safe development and use of AI models by introducing binding regulation on the handful of companies developing the most powerful AI models'.

Similarly, in its 'Make Work Pay'[13] document, also published prior to the election, the Labour Party pledged to 'protect good jobs, ensure good future jobs, and ensure that rights and protections keep pace with technological change'. It also committed to 'work with workers and their trade unions, employers and experts to examine what AI and new technologies means for work, jobs and skills, and how to promote best practice in safeguarding against […] algorithmic decision making'.

Furthermore, in the King's Speech in October 2024, it was stated that the Labour government would 'seek to establish the appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence models'.[14]

On the 13 January 2025 the UK government published its *AI Opportunities Action Plan* (the ***Action Plan***). The Action Plan contains recommendations to foster AI innovation in the UK which fall into the following categories:

- Support for innovators;
- Invest in making the UK a leading AI customer; and
- Attract global talent to establish AI companies in the UK.

In February 2025 the government declined to sign the *Statement on Inclusive and Sustainable Artificial Intelligence* at the Paris AI Summit (the ***Declaration***). Signatories to the Declaration pledged to make AI "*open, inclusive, transparency, ethical, safe, secure, and trustworthy"*.

As of May 2025 no government-backed UK AI Bill has been published. This lack of legislative prioritisation, together with the Action Plan and the UK's reticence to sign the Declaration may indicate that the UK Government's priorities on AI currently lie with business and innovation rather than regulation.

IV. USA

In October 2023, the Biden Administration issued an **executive order** on the '**safe, secure and trustworthy development and use of artificial intelligence**' (the ***Biden AI EO***).[15]

The Biden AI EO asserted that AI should not be used in ways that 'undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or

[11] 'Artificial Intelligence (Regulation and Employment Rights) Bill' (18 April 2024). https://www.tuc.org.uk/research-analysis/reports/artificial-intelligence-regulation-and-employment-rights-bill

[12] 'Change: Labour Party Manifesto 2024'.

[13] 'Labour's Plan to Make Work Pay: Delivering a New Deal for Working People', May 2024.

[14] The King's Speech 2024. https://www.gov.uk/government/speeches/the-kings-speech-2024

[15] 'Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence', 30 October 2023. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

cause harmful labor-force disruptions'. It set out several directives in relation to the labour market, including:

- within 180 days of the order:
  - Chairman of the Council of Economic Advisers to prepare a report on the potential impact of AI on the labour market;
  - Secretary of Labor to prepare a report identifying options to strengthen federal support for workers facing labour disruptions due to the adoption of AI and other technological advancements; and
  - Secretary of Labor to develop principles and best practices for employers to mitigate the potential risks AI poses to employee wellbeing and maximise its potential benefits, in consultation with unions and workers.
- within 365 days of the order:
  - Secretary of Labor to publish guidance for federal contractors regarding non-discrimination in hiring involving AI and other technology-based hiring systems to prevent unlawful discrimination from AI used for hiring.

As an executive order, the Biden AI EO was limited to the authorities of the executive branch and was not directly binding on private sector companies. Nevertheless, the Biden AI EO was a significant step towards potential regulation of the use of AI in the US.

In April 2024, federal agencies announced that they had completed all 180-day actions on schedule, and several issued guidance related to the above.

- The Department of Labor released guidance for employers stating that 'responsible human oversight' of AI is necessary to ensure that violations of federal labour law do not take place and that the risk of systemic bias is managed. In particular, the guidance states that things like keystrokes, blinking and internet monitoring, sometimes used by AI to monitor employees, are not dispositive when determining the number of hours worked.
- The Equal Employment Opportunity Commission released resources clarifying that existing law applies to the use of AI in the hiring and employment areas in the same way such laws apply to other more established employment practices.

1. Trump Administration Executive Order

The Biden AI EO was the first comprehensive step towards regulating the use of AI in the US, however, it remains unclear whether further regulation will follow as (i) meaningful AI legislation has not advanced beyond discussion in Congress and (ii) the Trump Administration has committed to repealing the 'dangerous Executive Order that hinders AI innovation' and ensuring that citizens have 'the right to self-custody of their Digital Assets' and can 'transact free from Government Surveillance and Control'.[16]

On January 23, 2025, The Trump Administration issued a new executive order, titled "Removing Barriers to American Leadership in Artificial Intelligence" (the "***Trump AI EO***"), which revoked the Biden AI EO and argued that the former had hampered the private sector's ability to innovate in the AI space by imposing overly burdensome government controls, and ordered federal departments and agencies to rescind any policies, regulations, orders and directives that are inconsistent with, or present obstacles to, enhancing the United States' leadership in this area.

The Trump AI EO also directed, within 180 days, the Assistant to the President for Science and Technology (***APST***), the Special Advisor for AI and Crypto, and the Assistant to the President for National Security Affairs (***APNSA***), in coordination with the Assistant to the President for Economic Policy, the Assistant to the President for Domestic Policy, the Director of the Office of Management and Budget and the heads of such executive departments and agencies as the APST and APNSA deem relevant, to develop an "AI Action Plan" to be presented to the president, with the goal of such plan being "to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security".

2. Employment-specific risks and regulation

In the absence of specific federal legislation on AI in the workplace, some states have enacted, or are considering, their own legislation. Some of these laws specifically tackle the use of AI tools in the employment context.

- **New York City:** in December 2021, New York City passed a law which requires employers to conduct bias audits of AI-enabled tools used for employment decisions and publish the results.[17] The law imposes notice and reporting obligations.

[16] 2024 GOP Platform: Make America Great Again!.

[17] 'Local Law to amend the administrative code of the city of New York, in relation to automated employment decision tools'. https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9

The law took effect on 1 January 2023 and entered into force on 5 July 2023.

- **Illinois:** the Illinois AI Video Interview Act tackles the use of AI in hiring.[18] The Act was amended in 2021 and went into effect in 2022. It requires employers using AI-enabled assessments to take various steps, including notifying applicants of AI use and obtaining their consent.
- **California:** the California Consumer Privacy Act (the ***CCPA***) gives consumers more control over the personal information businesses collect about them.[19] The definition of 'personal information' captures 'professional or employment-related information'. The CCPA also grants opt-out rights in relation to the use of automated decision-making technology, including profiling. The definition of 'profiling' captures a natural person's 'performance at work'.

V. Asia

Asian countries have generally adopted a lenient, voluntary approach to regulating AI - most of the major countries have issued guidelines instead of legally binding legislation.

China

In August 2023, the People's Republic of China's cyberspace security and internet content regulator (***CAC***) released provisional measures targeting content generation using generative AI, including text, images, audio and video.[20] These measures apply to any person utilising generative AI technology to provide services to the public in Mainland China, including those indirectly providing services through programming interfaces and APIs. The GenAI measures address issues such as the quality of training data, data privacy, intellectual property protection, fraud prevention, discrimination and bias, accuracy, algorithmic transparency, security, governance, and content moderation.

In January 2024, China's Ministry of Industry and Information Technology issued draft guidelines for standardising the AI industry.[21] The guidelines outline six major categories of standards essential for AI development in the country, including:

- **Safety Standards**, which regulate the safety requirements throughout AI technology, products, systems, applications, and services lifecycle. These include standards for basic safety, data, algorithm, and model safety, network and system safety, safety management and services, safety testing and assessment, safety labelling, content identification, product and application safety.
- **Governance Standards**, which regulate the technical research and operational service requirements of AI. These include technical requirements and evaluation methods for AI robustness, reliability, and traceability, as well as AI governance support technologies. They also standardise ethical governance requirements throughout the AI lifecycle, including ethical risk assessment, fairness and interpretability, technical requirements and evaluation methods for ethical governance, and AI ethical review standards.

Japan

Japan has no legally binding legislation that directly addresses AI. Instead, any restrictions are expected to be implemented through soft law rather than hard law for the time being. This relatively hands-off regulatory environment fosters an encouraging atmosphere for AI innovation and adoption.

In March 2019, the Japanese government published the **Social Principles of Human-Centric AI**.[22] These principles aim not to restrict the use of AI, but to uphold three core values: human dignity, diversity and inclusion, and sustainability through AI.

By 2023, the Ministry of Internal Affairs and Communications (the ***MIC***) introduced the 'AI R&D guidelines' and 'AI Utilization Guidelines'. Additionally, the Ministry of Economy, Trade and Industry (the ***METI***) issued the 'Governance Guidelines for Implementation of AI principles'.

In April 2024, the MIC and METI released the '**AI Guidelines for Business Ver1.0'**[23], replacing the previous three guidelines. These new guidelines take into account the development of AI technology and discussions on AI implementation over the past few years. They continue to emphasise the three core values established in the Social Principles of Human-Centric AI.

---

[18] 'Artificial Intelligence Video Interview Act'. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68

[19] 'California Consumer Privacy Act of 2018'. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[20] Provisional measures for the Management of Generative AI Services, 2023. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

[21] Basic security requirements for generative artificial intelligence service, 2024. https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/202311/7240bd43f3fc4b598351f9b135e68e4a.pdfhttps://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/202311/7240bd43f3fc4b598351f9b135e68e4a.pdf

[22] Social Principles of Human Centric AI. https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf

[23] AI Guidelines for Business Ver1.0. https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_9.pdf

To realise the three core values, the new guideline define ten general action points for AI developers, providers and business users:

- **Human-centric:** recognise the increasing risk of AI-generated disinformation, misinformation, and biased information and facilitating use of AI by the socially vulnerable;
- **Safety**;
- **Fairness:** minimise unfair, harmful, unconscious and/or potential bias;
- **Privacy protection**;
- **Security:** ensure AI confidentiality, integrity, and availability in line with the development of AI technology while countering AI system exploits;
- **Transparency**;
- **Accountability**: maintain ongoing information providing a dialogue with stakeholders, and frame AI governance and privacy policies;
- **Education/literacy**;
- **Fair competition**; and
- **Innovation**.

The Japanese government's '**Agile Governance**' approach involves a continuous and rapid cycle of activities, including environmental and risk analysis, goal setting, system design, operation, and evaluation, allowing multiple stakeholders to collaboratively drive governance practices. This collaborative approach has been yielding positive results. For instance, voluntary healthcare industry groups have developed sector-specific guidelines for AI providers, ensuring safe and secure AI services using generative AI in healthcare.

In end of May 2025, Japan enacted the Bill on the Promotion of Research and Development and Application of Artificial Intelligence-Related Technologies (the ***AI Bill***). The AI Bill focuses on promoting transparency rather than imposing strict regulations and is requiring businesses utilising AI to cooperate with government policies and investigations, with public "naming and shaming" as potential reputational consequence for non-cooperative businesses.

Singapore

While there is no specific AI regulation in force in Singapore, the Singapore government has taken proactive steps to address AI governance. In 2019, Singapore introduced its **Model AI Governance Framework**, which was updated in 2020.[24] The non-binding framework emphasises two key principles:

- the use of AI in decision-making process should be **explainable, transparent and fair**; and
- AI systems should be **human-centric**.

To support these principles, in May 2022, the Personal Data Protection Commission and the Infocomm Media Development Authority jointly launched 'AI Verify'. This initiative provides an AI governance testing framework and toolkit designed to help AI system developers and owners demonstrate responsible AI practices objectively. The toolkit includes technical and process checks that enable developers to self-assess and verify the claimed performance of their AI systems through standardised tests, although it does not define specific ethical standards.

In addition to regulatory frameworks, Singapore has also focused on preparing its workforce for the impact of AI. The introduction of 'A Guide to Job Redesign in the Age of AI' briefing[25], offers industry-neutral and practical guidance for organisations, assisting with their management of AI's impact on employees and the redesign of existing jobs to increase their value and harness the potential of AI. Central to this approach is ensuring that job redesign prioritises the dignity and wellbeing of employees, fostering a sustainable approach to integrating AI in the workplace.

On 30 May 2024, Singapore launched the Model AI Governance Framework for Generative AI[26], identifying nine dimensions to support a comprehensive and trusted AI ecosystem which include accountability and the use of third-party testing and assurance. This is the first comprehensive framework that consolidates different strands of global conversation surrounding AI governance.

India

India does not have specific AI regulations but it has introduced various initiatives and guidelines for the responsible development and deployment of AI technologies. Nevertheless, in 2023 the Indian Government enacted the Digital Personal Data Protection Act (***DPDP***),[27] which is likely to be used to address any AI wrongdoing relating to personal data until a specific AI regulation is introduced. The DPDP applies to the processing of digital personal data in India and beyond if such processing is connected with offering goods or services to data subjects residing in India.

On 1 March 2024, the Ministry of Electronics and Information Technology (the ***MeitY***) issued an

[24] Model Artificial Intelligence Governance Framework, second edition. https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

[25] A Guide to Job Redesign in the Age of AI. https://file.go.gov.sg/ai-guide-to-jobredesign.pdf

[26] Model AI Governance Framework for Generative AI. https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf

[27] Digital Personal Data Protection Act, 2023. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

advisory[28] (the ***1 March Advisory***) for intermediaries and platforms involved in the business of AI technology. The 1 March Advisory outlined key mandates, including (i) labelling any AI models that are under-testing or unreliable, and (ii) obtaining explicit prior approval from the government before deploying such models in India. Intermediaries were also instructed to comply with these requirements immediately and provide a report on action taken to the MeitY within 15 days.

Due to perceived ambiguities and compliance challenges with the 1 March Advisory, on 15 March 2024, the MeitY issued a new advisory[29] superseding the 1 March Advisory and removing certain compliance requirements, such as those related to government approval and submission of an action report. This potentially shifts India's regulatory approach from zero regulation to a more measured stance on AI regulation going forward.

In January 2025, Indian Ministry for Electronics and Information Technology released a report on 'AI Governance Guidelines Development'. Several recommendations in the report, if in fact operationalized, might deviate from the common refrain of a 'looser' regulatory approach for AI, which the government has been advocating for. However, the report also suggests several distinct regulatory approaches and also retains a broad refrain of 'voluntary' commitments.

VI. Recommendations for employers

Employers subject to the AI Act should take proactive steps to ensure their AI systems and practices comply. For example, they should consider taking the following steps:

- Review the AI systems already in use in the company to determine which of the risk categories they will fall into in the future.
- Depending on the identified risk potential, formulate guidelines for dealing with AI systems and integrate corresponding processes.
- Take the risk-based approach of the AI Act into account when planning and introducing new AI systems.
- In order to facilitate the introduction of new AI systems, develop a robust concept for the early involvement of any employee representative body where required.
- Appoint a representative for AI systems now and train them in accordance with the requirement for human supervision of AI systems.
- Offer training on basic technical understanding and responsible use of AI to the workforce.

Employers should also bear in mind that the use of AI may be restricted under **existing legislation**, such as in relation to equality, data protection, human rights and protection from unfair dismissal. For example, in the UK, a series of cases were brought under the GDPR by Uber drivers in relation to the use of automated processing to deactivate drivers' accounts. The Court of Appeal held that under the European Data Protection Board Guidelines, actual human intervention requires meaningful monitoring of decision-making carried out by someone who is competent and capable of changing the decision. Rubber stamping an automated decision would not meet these requirements.

VII. Conclusion and outlook

As we have noted, the current regulatory landscape is relatively varied as governments have taken different approaches to balancing innovation and regulation. However, the overarching theme across all jurisdictions is that any AI tool used must be **safe, fair, transparent and should have a human oversight** for the purposes of accountability.

The main risk for employers is ensuring that any AI tool used in recruitment, performance management, or any decision making process is unbiased. The best way to do this is by implementing effective human scrutiny of any output generated by AI and holding any relevant person accountable for any discriminatory output.

At present, the AI Act is the only robust and sweeping regulatory framework for the use of AI. However, as AI technology and systems become more advanced over time, further regulation will likely be required. Further to the AI Action Summit in France in February 2025, the dialogue between governments and tech companies about the need for regulation is expected to continue. Employers will, therefore, need to keep a close eye on the changing regulatory landscape in order to understand their liabilities and to ensure continued compliance across all relevant jurisdictions.

[28] Advisory No. eNo.2(4)/2023-CyberLaws-3. https://regmedia.co.uk/2024/03/04/meity_ai_advisory_1_march.pdf

[29] Advisory No. eNo.2(4)/2023-CyberLaws-3. https://www.meity.gov.in/writereaddata/files/Advisory%2015March%202024.pdf



Satya Staes Polet
Partner
T +32 477 96 11 29
E satya.staespolet
@freshfields.com



Takeshi Nakao
Partner
T +813 3584 8332
E takeshi.nakao
@freshfields.com



Sarah Rohmann
Global Head of Practice Development – P&R
T +49 211 49 79 453
E sarah.rohmann
@freshfields.com



Fan Li
Senior Associate
T +852 2913 2689
E fan.li
@freshfields.com



Rhianna Thornton-Reid
Associate
T +44 20 7716 4440
E rhianna.thornton-reid
@freshfields.com



David Mendel
Partner
T +44 20 7716 4586
E david.mendel
@freshfields.com



Stephanie Chiu
Counsel
T +852 2846 3491
E stephanie.chiu
@freshfields.com



Olga Chislova
Senior Associate
T +44 20 7716 4539
E olga.chislova
@freshfields.com



Chaim Leggiere
Associate
T +1 212 230 4630
E chaim.leggiere
@freshfields.com



Jordan Riley
Associate
T +1 646 23 1 7049
E jordan.riley
@freshfields.com

freshfields.com

This material is provided by the international law firm Freshfields Bruckhaus Deringer LLP (a limited liability partnership organised under the laws of England and Wales authorised and regulated by the Solicitors Regulation Authority (SRA no. 484861)) and associated entities and undertakings carrying on business under, or including, the name Freshfields Bruckhaus Deringer in a number of jurisdictions, together referred to in the material as 'Freshfields'. For further regulatory information please refer to www.freshfields.com/support/legal-notice.

Freshfields Bruckhaus Deringer has offices in Austria, Bahrain, Belgium, China, England, France, Germany, Hong Kong, Ireland, Italy, Japan, the Netherlands, Singapore, Spain, the United Arab Emirates, the United States and Vietnam.

This material is for general information only and is not intended to provide legal advice.

© Freshfields Bruckhaus Deringer LLP 2025