MANAGING THE MACHINE

How we regulate AI as it handles HR decisions

Global HR Lawyers
Ius Laboris

Global HR Lawyers
Ius Laboris

Ius Laboris is a leading international employment law practice combining the world's leading employment, labour and pension firms. With an unsurpassed geographic coverage of 57 countries, Ius Laboris lawyers help clients navigate the world of HR law every day.

Nothing in this publication should be treated as an authoritative statement of the law and the opinions expressed should not be taken as fact. This report should in no circumstances be relied upon without first taking legal advice.

IUS LABORIS

Ius Laboris is consistently recognised as the leading legal service provider in employment, immigration and pensions law. With a global reach across 57 countries in Europe, the Americas, the Middle East and Asia, our alliance of law firms assists international employers in navigating the complexities of the modern workplace with ease and confidence.

Founded in 2001 by a group of labour and employment lawyers from Belgium, France, Spain, Luxembourg and Italy, Ius Laboris has since expanded its reach to cover 57 countries worldwide. Throughout our journey, we have consistently earned recognition as the premier legal service provider in our field, offering unparalleled expertise and support to our clients.

Ius Laboris has nine active and dynamic Expert Groups, gathering members from diverse regions and disciplines within employment, immigration and pensions law. These groups blend expertise and experience from across the globe to meet workplace challenges and offer innovative solutions to employers.

To analyse and propose solutions on emerging employment-related issues, Ius Laboris also has an International Policy Group. Comprising thought leaders from across our network, this group engages in in-depth discussions on key HR law matters, providing policy recommendations to major institutions and valuable insights for employers worldwide.

This report is the result of collaboration between some of our experts from within the alliance and our central team.

OUR EXPERTISE

DATA PRIVACY
DIVERSITY & INCLUSION
INDIVIDUAL EMPLOYMENT RIGHTS
HEALTH & SAFETY
IMMIGRATION & GLOBAL MOBILITY

Local experts, global reach in 57 countries

OUR EXPERTISE

INVESTIGATIONS

PAY, BENEFITS & TAX

PENSIONS

RESTRUCTURING & LABOUR RELATIONS

TABLE OF CONTENTS

FOREWORD BY BURKARD GÖPFERT

Burkard Göpfert
Partner, Ius Laboris Germany

Globally we appear to be entering a new phase of Artificial Intelligence, shifting rapidly from experimentation with the technology to more widespread commercial deployment. This is particularly visible in the workplace. Employers are increasingly adopting AI tools to support HR functions such as recruitment, performance management and workforce planning. This marks a fundamental shift in how HR decisions at work are made, understood and challenged, with an ever-greater reliance on automated, AI-driven outputs.

Yet while businesses accelerate adoption, policymakers around the world are racing to keep pace. They face difficult questions that will shape the conditions under which AI is used at work. Central among them is the challenge of striking the right balance: encouraging innovation, while safeguarding workers' rights and opportunities.

To better understand whether countries are achieving this balance we conducted a survey of experts across 29 of our Ius Laboris firms, examining the approaches being taken to regulate the use of AI in the workplace. What becomes clear from our data is that across jurisdictions, even as regulatory methods diverge, the same challenges arise from regulating AI at work - transparency, accountability, explainability, contestability, bias mitigation and protection for independent contractors, to name a handful. Set against the wider backdrop of shifting global regulatory dynamics, the question becomes: what solutions are both effective and workable?

In the following report, we begin with an economic analysis exploring key statistics on the scale and speed of AI adoption, and how businesses and society are responding to this. Then, we highlight some key cross-border trends emerging from our survey, followed by an in-depth analysis of the data collected. This is divided by region and structured in each one as follows:

- the current landscape;
- where regulatory gaps and challenges persist; and
- how those gaps might be addressed.

We close with reflections from our experts in three interview pieces that also include practical guidance for employers navigating this fast-moving landscape.

By bringing these perspectives together, we aim to support employers, policymakers and practitioners as they navigate this complex and rapidly evolving area of AI in the workplace.

For a long time, AI was something most people rarely thought about. It worked quietly in the background, supporting systems and processes without drawing much attention. It was not part of everyday routines or daily conversations. That began to change with the arrival of ChatGPT and other generative AI tools. Suddenly, AI became visible. People could interact with it directly, ask questions and use it in ways that felt personal. Although the technology had been developing for decades, this moment marked a clear shift. Awareness finally caught up with progress, and AI moved into the mainstream.

Today, AI tools influence how people communicate, access information and navigate both their personal and professional lives. What once felt like a technical experiment is now part of everyday routines. Unsurprisingly, AI has rapidly moved to the centre of policy debates. How this technology shapes society will depend not only on the pace of innovation, but also on the governance choices made - including the rules that determine how AI is used in workplaces.

Before turning to employment-related AI regulations and policies across countries, it is worth, however, pausing to understand the scale and pace of AI adoption, and how businesses and society are responding to this progress.

01

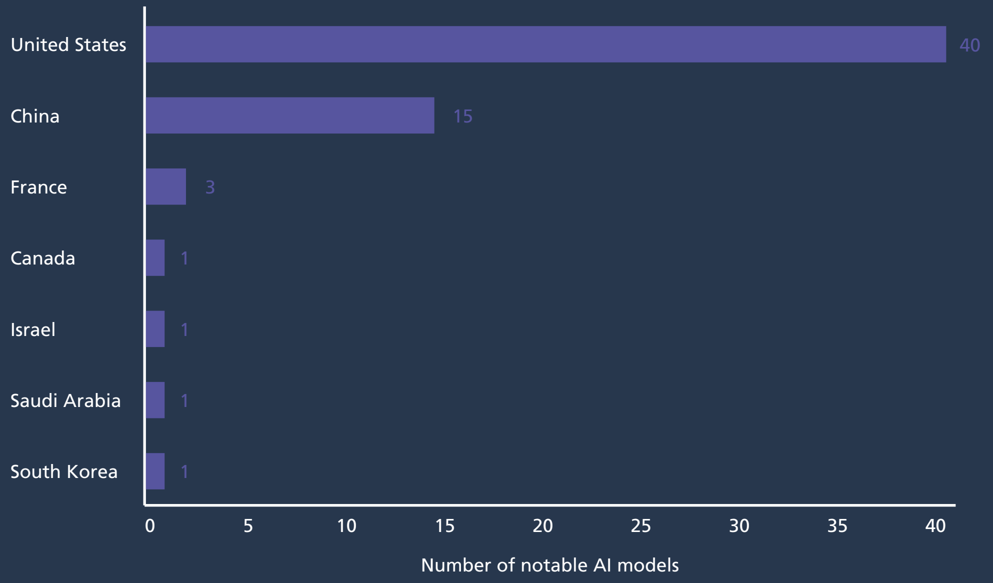
THE SCALE AND SPEED OF AI ADOPTION

WHO LEADS THE MARKET?

The recent surge in AI visibility is closely linked to developments in 2022 and 2023, when widely accessible generative models brought AI into everyday use. These years saw a rapid expansion in the number of high-profile AI systems. The US emerged as the most active hub, followed by China, while European contributions were more limited in scale.

In 2024, fewer major models were introduced across regions, including the US, China and Europe. While innovation continued, the pace of headline releases eased compared to the previous year (2025 AI Index report). This is likely the result of several overlapping factors. As models become larger and more complex, development cycles are expanding, and resource requirements are increasing. At the same time, advancing the frontier of AI has become more challenging, as gains now depend on more sophisticated approaches, rather than incremental improvements. Together, these dynamics help explain why growth in new model launches has slowed, even as AI continues to deepen its presence

Figure 1: Number of notable AI models by select geographic areas, 2024

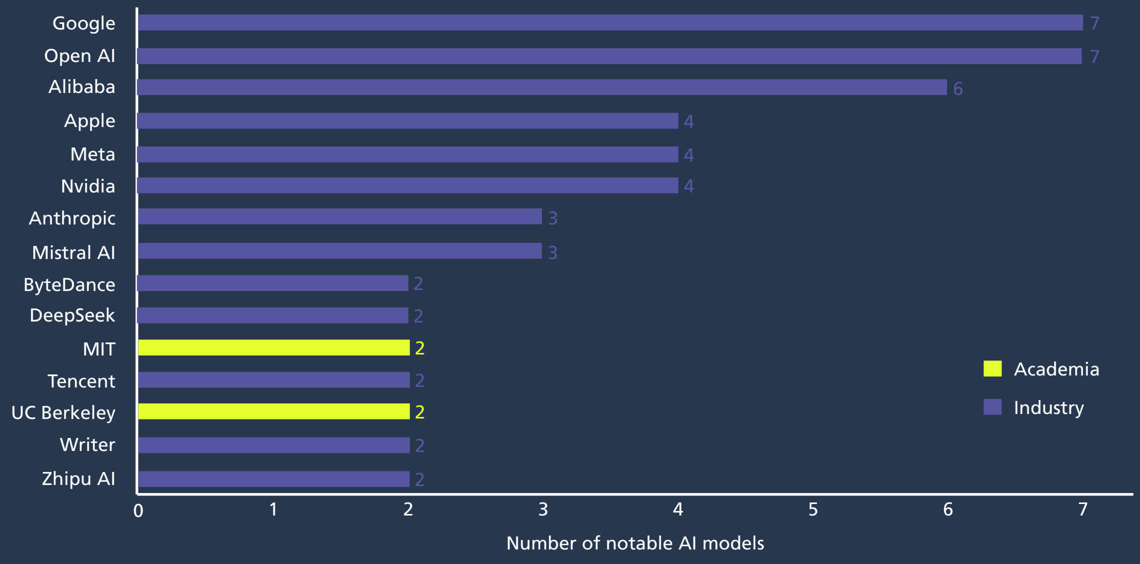


Source: Epoch AI, 2025 | Chart: 2025 AI Index report

across society and the economy.

A clear shift is visible in terms of where notable AI models are being developed. In the earlier phases of modern machine learning, universities were at the forefront. Until around 2014, academic institutions produced most of the models. Since then, leadership has moved decisively towards industry. Large technology companies now drive the majority of high-impact AI systems. Over the past decade, the share of notable models originating from industry reached more than nine tenths of total output. In 2024, Google and OpenAI were the most active contributors, followed by Alibaba, Apple and Meta (2025 AI Index report).

Figure 2: Number of notable AI models by organisation, 2024



Source: Epoch AI, 2025 | Chart: 2025 AI Index report

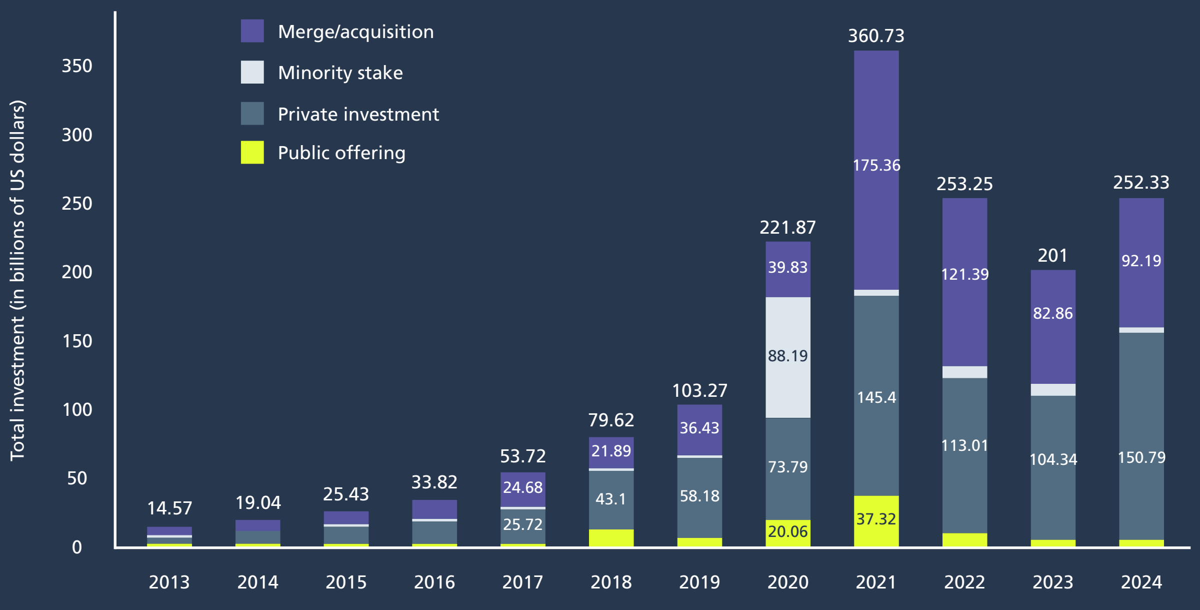
HOW BUSINESSES RESPOND TO AI

Global corporate AI investment has risen steadily over the past decade, covering everything from private funding to mergers and acquisitions. In 2024, it reached USD 252.3 billion, almost thirteen times higher than it was a decade ago. The largest increase came from private investment, with more capital flowing into privately-held AI companies. Activity in mergers and acquisitions also rose significantly.

On the other hand, the use of AI in business is also growing rapidly. According to the latest McKinsey report (McKinsey & Company Survey, 2024), 78% of respondents indicate that their organisations are now using AI in at least one business function, up from 55% in 2023.

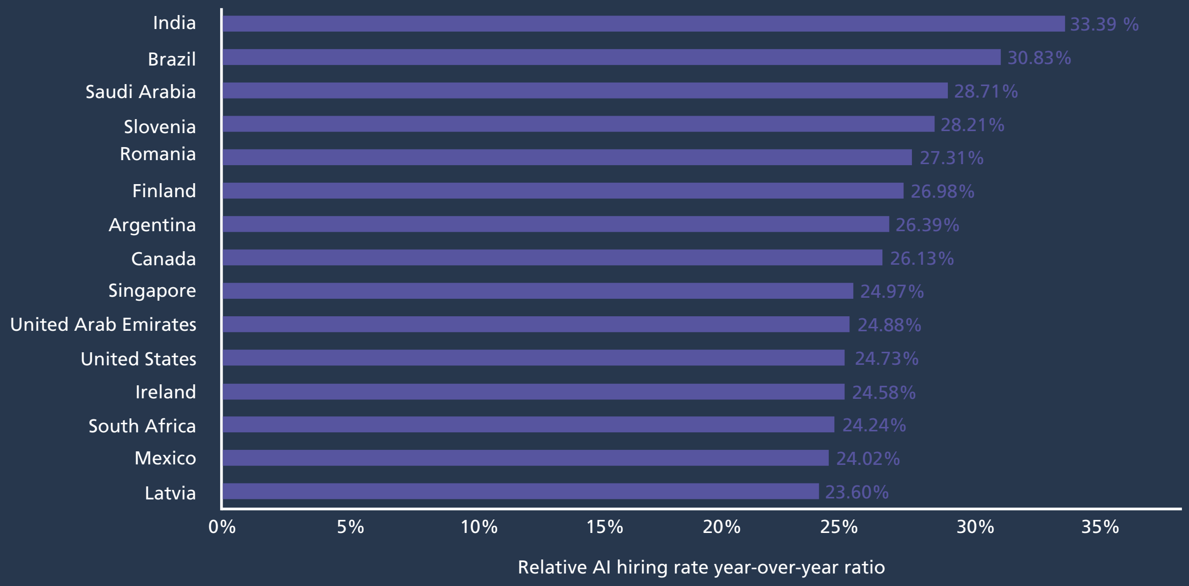
Companies aren't just putting money into AI, they're also on the lookout for talented AI professionals. In 2024, the fastest-growing markets for AI hiring were India, Brazil and Saudi Arabia (2025 AI Index report).

Figure 3: Global corporate investment in AI by investment activity, 2013 – 24



Source: Epoch AI, 2025 | Chart: 2025 AI Index report

Figure 4: Relative AI hiring rate year-over-year ratio by geographic area, 2024

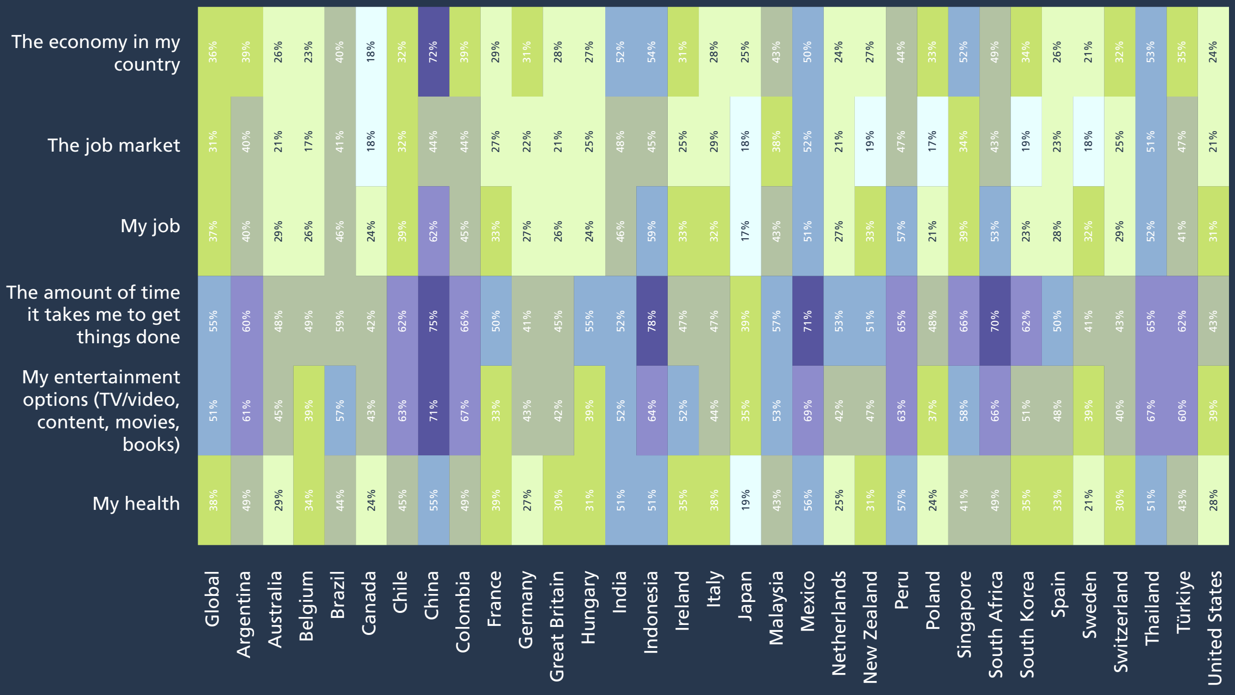


Source: LinkedIn, 2024 | Chart: 2025 AI Index report

DO PEOPLE TRUST AI?

People around the world are growing more positive about AI, but big differences remain between regions. In countries such as China (83%), Indonesia (80%) and Thailand (77%), most people see AI products and services as more helpful than harmful. Meanwhile, optimism is much lower in places such as Canada (40%), the US (39%) and the Netherlands (36%). Still, attitudes are changing. Since 2022, several countries that were more sceptical have seen a noticeable rise in positivity, including Germany, France, Canada, the UK and the US (2025 AI Index report).

Figure 5: Global opinions on the potential of AI to improve life by country, 2024



Source: Ipsos, 2024 | Chart: 2025 AI Index report

INTERNATIONAL COOPERATION ON AI GOVERNANCE

As trust in AI increases and AI products become more sophisticated over time, international cooperation on AI governance is also expanding. The OECD has updated its AI Principles and refined its framework to reflect recent developments in AI governance. These principles promote inclusive growth, transparency and explainability while upholding the rule of law, human rights and democratic values (OECD/LEGAL/0449).

The Council of Europe has adopted a legally binding AI treaty, the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). During the United Nations Summit of the Future on 22 September 2024, global leaders approved the Pact for the Future, including its annexes: the Global Digital Compact and the Declaration on Future Generations (Resolution A/RES/79/1). Among other commitments, participants agreed to strengthen international governance of artificial intelligence for the benefit of humanity.

The G7 Digital Competition Communiqué reaffirmed commitments to fair and open AI markets and highlighted the need for coordinated regulatory approaches. Earlier discussions focused on competition issues and the regulatory challenges created by the rapid expansion of AI. In addition, the first International Network of AI Safety Institutes has been established, bringing together nine countries and the EU to formalise global cooperation on AI safety. The network connects technical organisations working to assess the risks of advanced AI systems, support governments and societies, and develop practical safety solutions.

As AI technologies become increasingly embedded in both business operations and daily life, their impact on workplaces is becoming more visible and, in many cases, more complex. Companies are using AI to streamline workflows, manage performance, recruit and train staff and make decisions that shape employees' day-to-day work. Governments and policymakers are responding to this new reality by revising the existing regulatory frameworks. In the following section, we will explore how different countries are addressing these challenges and examine the current state of AI workplace regulations.

02 COMMON CHALLENGES UNDER DIFFERENT SKIES

In this next section of the report, we explore three questions: first, how are countries currently regulating the use of AI in the workplace (**the landscape**); second, what are the key challenges for policymakers (**the challenges**); and third, how can countries resolve these challenges (**the solutions**). Across the three regions we surveyed, clear cross-cutting themes emerge in response to each of these questions.

The regulatory **landscape** is diverse, with notable jurisdictional nuances, yet clear patterns are evident. One consistent thread across all regions is that countries continue to rely on familiar foundations when it comes to regulating AI in the workplace: established employment and data-protection frameworks. Alongside this shared baseline, three distinct regulatory approaches take shape. First, there are the rules-based, prescriptive regimes - most prominently in the EU and increasingly mirrored in new initiatives across the Americas region. Then we have more guidance driven approaches found elsewhere in Europe and the Middle East, as well as in parts of the Asia-Pacific region. Finally, the United States continues to have a fragmented state and local level patchwork, despite pressure at a federal level.

The **challenges** of regulating workplace AI overlap significantly when it comes to ensuring adequate protection for employees and independent contractors. While there is a sense that existing frameworks provide meaningful safeguards in many countries, important gaps and limitations remain. To demonstrate the extent of this 'overlap', of the gaps referenced by our respondents, only three appeared in a single jurisdiction; all other issues surfaced in multiple countries. The most common challenges cited relate to the transparency and explainability of automated decisions, accountability and contesting an automated decision, and the closely related risk of biased decision-making and discrimination. Specific vulnerabilities for independent contractors were also highlighted by several respondents. Although this challenge stems less from AI deployment and more from worker-classification rules, it remains an important consideration in the wider discussion of AI in the workplace.

Finally, the **solutions** highlighted by respondents vary, yet distinct trends emerge. Some countries favour the introduction of specific binding rules on AI, though views differ on whether these should take the form of comprehensive frameworks or more targeted legislative measures. In jurisdictions where such rules already exist, there is a sense that more time is needed to observe how current frameworks operate in practice and how effectively they are enforced before introducing further measures. Others emphasise the value of non-binding tools such as guidance and sectoral standards, although some respondents caution that these instruments lack enforceability and can lead to uneven adoption, meaning they are best positioned to complement, rather than replace, binding guardrails. And, notably, some respondents take the view that no further intervention is required at all.

Despite the diversity of regulatory approaches then, these findings show that countries are ultimately grappling with many of the same core issues - common challenges arising under very different skies. With signs of convergence around certain solutions, it will be interesting to see how the landscape develops.

EUROPE AND THE MIDDLE EAST

The current regulatory approach in the EU can be described as prescriptive and rules-based, underpinned by the EU AI Act which establishes a risk-based AI classification system for AI tools, as well as a separate set of rules for certain types of AI models (which effectively power those tools). AI tools used in the workplace will likely be categorised as 'high-risk' meaning employers who provide or deploy such tools will be subject to various obligations under the legislation.

The EU-based firms that we surveyed generally appear satisfied with the current regulatory landscape, when accounting for the phased implementation of the EU AI Act, and the fact that we are still in the early stages of widespread commercial AI development and its use in the workplace. There is a sense that more time is needed to review the practical application and enforcement of existing frameworks, before introducing new ones.

This 'need for more time' may be amplified further if recent proposals to simplify the EU's digital rulebook (which would involve amending the GDPR and AI Act) are passed. The proposals are significant and represent pressure to shift the EU's approach to one that is clearer and more innovation-friendly.

Outside of the EU, EME-based firms describe a varied regulatory landscape: while some jurisdictions have specific AI laws in force (or under development), others place a greater focus on non-binding guidelines and principle-based approaches. In practice though, there is a suggestion that some employers in the region are already converging around EU-style guardrails as a gold standard – evidence perhaps of the 'Brussels effect' being in play.

EUROPE AND THE MIDDLE EAST

THE EUROPEAN UNION

THE CURRENT REGULATORY LANDSCAPE

Most EU countries regulate workplace AI through a combination of EU and domestic legislation. While non-binding instruments exist, they tend to play a secondary role and are seen as being less influential than in other regions we surveyed (most notably, the APAC region). Below, we examine:

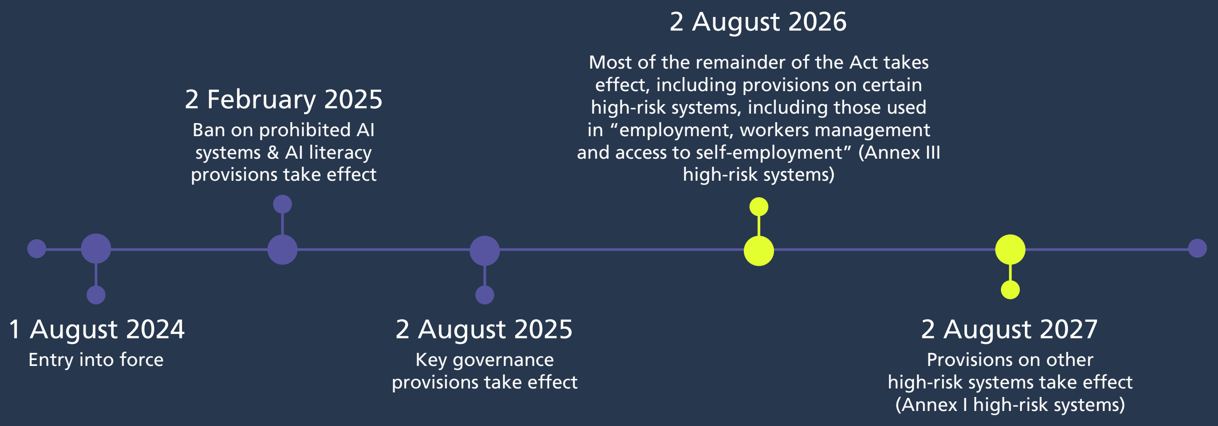
1. what is in place now at EU-level;
2. proposed amendments to that framework that may or may not take effect at a later date; and
3. how domestic frameworks are taking shape.

1. EU legislation: Central to the AI policy puzzle

Labelled the "world's first comprehensive AI law",[1] the EU's regulatory anchor is its Artificial Intelligence Act (Regulation (EU) 2024/1689) (the 'EU AI Act') which formally entered into force in 2024 and is being implemented on a phased basis (see Figure six below). Being an EU Regulation, the EU AI Act is directly applicable in all EU Member States and introduces tangible enforcement mechanisms, including significant administrative fines proportionate to global turnover in cases of non-compliance.

Unsurprisingly, the Act is referenced in most, if not all the survey responses from our EU-based firms, and exemplifies the EU's current preference for a more prescriptive, rules-based regulatory model, introducing detailed

Figure 6: Current implementation timeline, EU AI Act


2 August 2026
Most of the remainder of the Act takes effect, including provisions on certain high-risk systems, including those used in "employment, workers management and access to self-employment" (Annex III high-risk systems)
2 February 2025
Ban on prohibited AI systems & AI literacy provisions take effect
1 August 2024
Entry into force
2 August 2025
Key governance provisions take effect
2 August 2027
Provisions on other high-risk systems take effect (Annex I high-risk systems)

legal obligations rather than broad, guiding principles.

While the EU AI Act does not exclusively regulate the use of AI at work, it will have implications for employers in the region and meaningfully impact workplace practices. Below, we summarise some of the headline points.

- **High-risk systems:** The Act establishes a risk-based framework for regulating AI systems, dividing these into four categories – 'unacceptable' risk, 'high' risk, 'limited' or 'transparency' risk (i.e. AI systems with specific transparency issues), and 'minimal' risk. Provisions under the Act on high-risk systems, which includes those involved in the context of employment and the management of workers (e.g. CV-sorting software for recruitment), will apply from 2 August 2026. Many employment related use cases will fall into the high-risk category.
- **Employers as 'deployers':** The Act distinguishes between different types of organisations, most commonly 'providers' and 'deployers'. Different obligations extend to both. Employers could be classified as either, with deployers facing obligations in relation to the use of high-risk AI systems, such as ensuring proper use, monitoring, and informing workers about AI interactions. Providers, including those who modify AI systems or brand them, must implement rigorous risk management systems, oversee data usage, maintain logs, and register with the EU database.
- **AI literacy:** Providers and deployers must also ensure that their staff and others dealing with the operation and use of AI systems on their behalf have a sufficient level of AI literacy. This applies to any AI system caught by the Act, irrespective of the level of risk. Since employers are typically the deployers of AI systems, they are responsible for ensuring that their employees have the necessary competence in using AI.
- **Prohibited AI:** The Act has already banned the use of prohibited AI systems. This includes the use of AI systems intended to be used to detect the emotional state of individuals in situations related to the workplace.

The European AI Office and the national authorities are responsible for implementing, supervising and enforcing the Act. To this end, the Act requires Member States to establish or designate:

- as **national competent authorities**, at least one notifying authority and at least one market surveillance authority to ensure the application and implementation of the Act; and
- **fundamental rights protection authorities**, which will receive additional powers to ensure they can fulfil their mandate in relation to the use of high-risk AI systems.

Throughout 2025, Member States designated various enforcement bodies ready for the coming into force of the Act's enforcement provisions on 2 August 2026. Even so, progress on designation has been uneven. All 27 Members States have now identified fundamental rights protection authorities, however only nine have also officially designated national competent authorities. A further nine have signalled forthcoming designation (i.e. according to a draft legislative proposal or official confirmation), while the remaining Member States have yet to identify their national competent authorities.[2] We also see considerable variation between countries regarding the total number of designated authorities.

In addition to the EU AI Act, the EU's General Data Protection Regulation ('GDPR') is also referenced in most responses we received from our EU-based firms. Although the GDPR does not specifically tackle the use of AI at work, it contains provisions that are relevant, including on automatic decision making (including profiling) and transparency.

However, readers should note that this framework may evolve, as the EU explore reforms aimed at easing compliance burdens and creating a more simplified regulatory landscape. We explore this next.

2. The 'Digital Omnibus': Is simplification on the horizon?

Before we examine the local regulatory landscapes within the EU, it is important to highlight the recent and ongoing attempts by the EU Commission to simplify the EU's existing digital rulebook, including the GDPR and EU AI Act. While these are proposals at this stage and will follow the usual EU legislative processes, they highlight the wider regulatory tension facing policymakers between erecting robust safeguards and the need to drive innovation.

In January 2025, the European Commission presented its so-called 'competitiveness compass', a "new roadmap to restore Europe's dynamism and boost [its] economic growth." As part of this initiative, which follows Mario Draghi's report on Europe's competitiveness,[3] the Commission advanced 'omnibus proposals' aimed at simplifying certain EU legislation. One of these, the 'Digital Omnibus' proposal published on 19 November 2025, focuses on simplifying the EU's digital rules and regulations.

The 'Digital Omnibus' proposal includes two parts: a 'Digital Omnibus Regulation Proposal' focused on targeted amendments to the EU's data protection and privacy rules, including provisions in the GDPR; and a 'Digital Omnibus on AI Regulation Proposal' which is more narrowly targeted at the EU AI Act. Key proposals that might impact the use of AI at work if adopted can be summarised as follows:

'Digital Omnibus on AI Regulation Proposal'

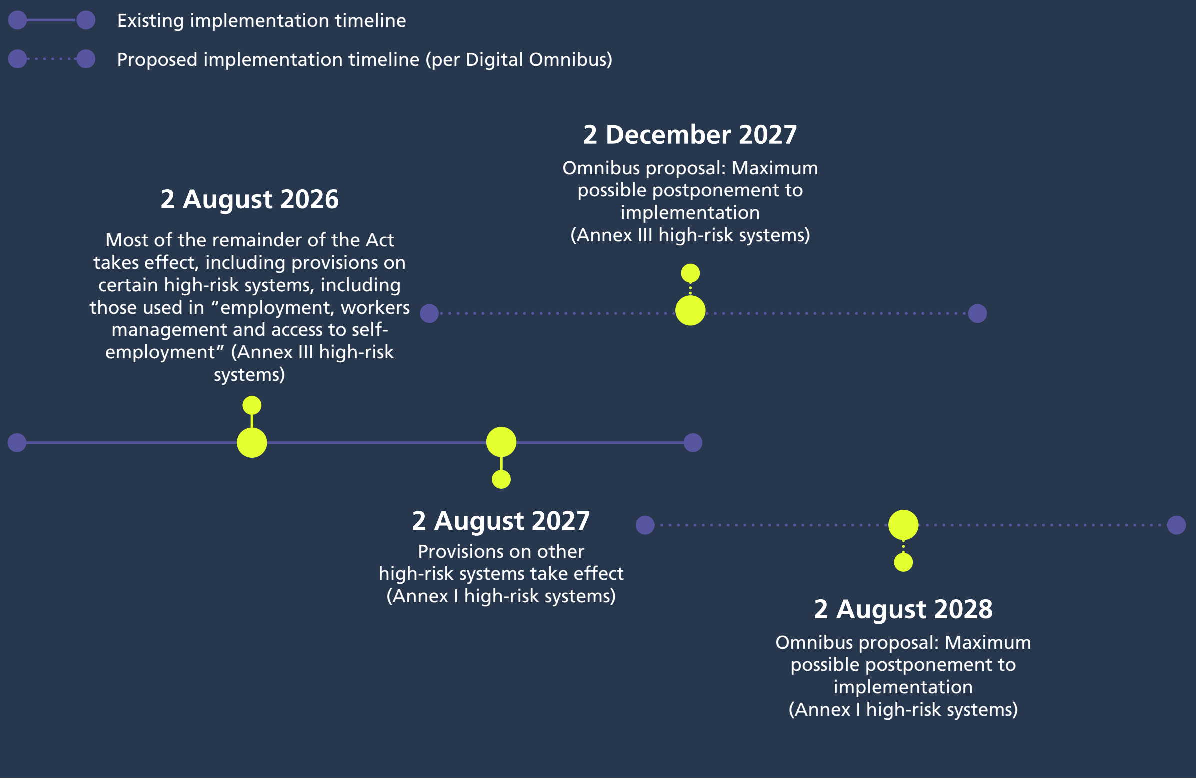
- **Delay to AI Act implementation -** One of the standout proposals is linking the application of the rules for high-risk AI (which is likely to include many HR AI systems) to the availability of support tools (such as standards and guidelines) by adjusting the timeline for such application (see figure seven). The proposals would mean that the rules for high-risk AI systems will apply a maximum of 16 months later than originally envisaged. This proposal acknowledges the "challenge that the delay of standards and other support tools cause for the implementation of the AI Act".
- **Supporting compliance** – Another key proposal would allow providers and deployers to process special categories of personal data to ensure bias detection and correction, subject to appropriate safeguards. The Digital Omnibus also proposes broadening the use of AI regulatory sandboxes and real-world testing so that more innovators can benefit from these tools (including setting up an EU-level regulatory sandbox from 2028).
- **Simplification** – The proposals would also extend simplified technical documentation to SMEs and mid-cap companies; mandate the Commission and Member States to promote AI

literacy and provide ongoing support; remove the obligation for a harmonised post-market monitoring plan to allow flexibility; and reduce registration burdens for AI systems performing non-high-risk tasks within high-risk sectors.

‘Digital Omnibus Regulation Proposal’

- **Use in AI development** – The development of AI systems and models may involve the collection of large amounts of data, including special category data. To avoid hindering AI innovation, the proposal introduces an exception to the general prohibition on processing special category data where such data forms part of and remains in the “training, testing or validation data sets” of the AI system or model. This would be subject to the controller implementing “appropriate technical and organisational measures”.
- **Lawful basis for processing data** - The proposal sets out that “legitimate interest” will be explicitly codified as a lawful basis for processing personal data for the development and operation of AI models and systems, provided that appropriate safeguards are in place.
- **Requirements for automated decision making** - The proposal aims to clarify Article 22 of the GDPR to provide “greater legal certainty” for decisions made through automated decision

Figure 7: proposed changes to implementation timeline, EU AI Act


Existing implementation timeline
Proposed implementation timeline (per Digital Omnibus)
2 December 2027
Omnibus proposal: Maximum possible postponement to implementation (Annex III high-risk systems)
2 August 2026
Most of the remainder of the Act takes effect, including provisions on certain high-risk systems, including those used in “employment, workers management and access to self-employment” (Annex III high-risk systems)
2 August 2027
Provisions on other high-risk systems take effect (Annex I high-risk systems)
2 August 2028
Omnibus proposal: Maximum possible postponement to implementation (Annex I high-risk systems)

making. It clarifies that when deciding if an automated decision is necessary for "entering into, or performance, of a contract" it does not matter if the decision could be taken otherwise than by solely automated means. The idea is to make it easier to rely on the necessary for performance of a contract basis for automated decision-making usage.

It is important to note that, as proposals, these will be subject to change. Regardless, they demonstrate an interesting tension with the EU's current approach to regulating AI: pulling one way is the more prescriptive, rules-based model that the EU AI Act embodies (and that is supported by the GDPR); and pulling the other is pressure for the EU to restore its dynamism and competitiveness on the global stage with more 'innovation-friendly' rules on AI.

This connects with another, broader theme, with some commentators suggesting that the proposed simplification has been influenced by global regulatory power-dynamics and the emergence of a so-called 'Washington effect'.[4] Many will have heard of the 'Brussels effect' which refers to the EU's unilateral power to regulate global markets, whereby market forces alone are often sufficient to convert the EU standard into the global standard as multinational companies voluntarily extend the EU rule to govern their global operations.[5] In a similar sense, the 'Washington effect' describes the US federal government, under the influence of Big Tech, centralising AI regulation by proposing to pre-empt certain state laws and pressuring foreign regulators, including the EU, to ease up on US companies. This appears to be the goal of the current US administration against the development of state and local level AI regulation (as we explore below). If successful, some consider the net effect to be an increasing concentration of regulatory power on AI in the US federal government's executive branch.[6]

Parallel to this, it could also be argued that there is a soft 'UK effect' in-play here, given that some of the proposed changes in the Digital Omnibus (around automated decision-making, for example) would more closely align the EU's position to that of the UK. It is noteworthy that, despite the changes to automated decision-making in the UK's Data (Use and Access) Act 2025 (relaxing the rules), the EU still renewed the UK's data adequacy decisions in December 2025.

Others suggest that the 'Brussels effect' still applies to some extent. In fact, our UK firm note in their survey response that organisations may still adopt the EU AI Act as part of internal governance as a global gold standard for AI compliance, even when not legally required. This would reflect similar past practices with data protection regulation as employers seek to avoid implementing different AI policies to fit different jurisdictional frameworks. From a different, yet connected perspective, countries in the Americas are proposing frameworks heavily inspired by the principles and provisions of the EU AI Act (see below).

Regardless of which 'effect' is winning or losing, the coming months will reveal how these Digital Omnibus proposals evolve through the EU's legislative process.

3. Local frameworks

At a local, Member State level, we see some Member States introducing specific AI legislation to operationalise and/or complement the EU framework set out previously, although the majority rely on existing employment rights and data protection legislation. Non-binding instruments such as guidance, standards and voluntary codes are currently less prominent than in other regions.

Specific-AI legislation

The EU AI Act is directly applicable, meaning it forms part of the national law of each member state without the need for any domestic implementing legislation. Even so, the Act does require Member States to take steps to operationalise its provisions. To this end, three of the 14 EU-based firms we surveyed confirmed that their countries have introduced specific AI legislation aimed at implementing and complementing the EU AI Act (**Denmark, Finland and Italy**). Several others have either published or are preparing draft implementing legislation. As noted, enforcement bodies have also been established across the region.

Beyond these EU-wide measures, several Member States have introduced additional national provisions to address AI-specific challenges in the workplace. **Germany** stands out in our survey as having made targeted legislative amendments to introduce specific AI obligations in relation to works councils. The Works Council Modernisation Act 2021 makes several amendments to the existing co-determination framework so that this now explicitly addresses some of the challenges with AI. In particular, works councils must now be informed about the planned use of AI in a company, followed in most cases by a period of consultation.

Elsewhere - and linking with the theme of AI and collective workplace rights - **Poland** has proposed a draft bill to amend its Trade Unions Act. This would entitle trade unions to obtain information from the employer about the parameters, rules, and instructions underlying the algorithms or AI systems that influence decisions affecting working and pay conditions.

Finally, in **Bulgaria**, the Labour Code now requires that, when employers use an information system for algorithmic management of remote work, they must inform employees in writing about how decisions are made. Additionally, at the employee's written request, the employer (or its designated official) must review any algorithmic decision and communicate the final outcome to the employee.

Our firm in **Denmark** indicates that such targeted legislation may become necessary should time and experience demonstrate that existing instruments fail to ensure adequate protection.

Existing employment rights legislation

Beyond specific AI legislation, for 12 of the 14 EU-based firms we surveyed existing employment rights legislation currently forms part of their regulatory landscape when it comes to the use of AI at work. Five cite individual employment rights frameworks (including equality, general employment and health and safety legislation), four cite collective employment rights frameworks and three reference both types. Data protection legislation also features in several answers received from our EU-based respondents.

Finland provides a particularly strong example where existing employment laws are seen to protect workers from harmful AI use. Key statutes such as the Employment Contracts Act, Non-discrimination Act, and Equality Act prohibit discriminatory practices, while the Co-operation Act requires employers to notify and consult employees on workplace policies, technical monitoring, and employment changes linked to AI adoption.

In other cases, existing frameworks are described as 'technology-agnostic' such that liability under, for example, existing equality legislation, attaches to the employer and not the technology. As our firm in **Denmark** notes, employers will be responsible for discriminatory or otherwise unlawful decisions in employment relationships no matter whether made through AI tools provided by a third party or not.

These measures illustrate how existing frameworks can effectively mitigate AI-related risks without the need for entirely new legislation.

How do non-binding instruments fit in?

Guidance, industry standards or voluntary codes of practice do not feature as centrally in the EU as they do in other regions that we surveyed. They are not viewed as being less important or relevant; they just appear to be less influential to the wider regulatory landscape at this stage.

Of the 14 EU-based law firms surveyed, only two refer to existing non-binding instruments (**Denmark** and **Germany**). Even so, and although in Germany the use of non-binding instruments is possible, the scope of application in this context is limited by the co-determination of the works council. If there is a works council - and in line with the German legislation highlighted above - the provisions of the Federal Ministry of Labour and Social Affairs' guidelines on the use of AI in the administrative practices of labour and social services can only be implemented if the works council agrees to them.

That notwithstanding, and with the phased implementation of the EU AI Act ongoing, the number of Member States adopting national guidance and other non-binding instruments is expected to increase. This also doesn't account for the EU-level guidance that has been published.

IS THE CURRENT LANDSCAPE ADEQUATE?

As part of our survey, we wanted to get a sense of the extent to which the current regulatory landscape in the EU (and in the other regions covered below) is viewed as adequately protecting employees and self-employed contractors when employers use AI or algorithmic management tools at work. Are current rules sufficient, or are there regulatory gaps that need to be addressed? Should the focus be on new legislation, non-binding guidance, or simply allowing time for existing frameworks to adapt and be tested in practice?

Across our EU-based firms surveyed, three firms expressly indicated that there were no obvious gaps in their countries' existing regulatory approach (**Bulgaria**, **Croatia** and **Finland**). Our firm in **Finland**, for example, considers that the existing Finnish legal framework described above should "quite extensively" protect employees against the harms of workplace AI. Therefore, it is not clear whether, in their view, there is a necessity for new AI-specific legislation (including the new EU AI Act) to apply in the context of employment.

The remaining 11 respondents outlined, to varying degrees, potential gaps in their current regulatory framework and the protections afforded to employees and self-employed contractors. For example, our **Danish** firm suggested that the overall framework is "capable of covering most foreseeable risks"; our firm in **Greece** references a "meaningful" level of protection; our firm in **Sweden** a "basic" level; and our firm in **Poland** a "partially and highly uneven" level.

Importantly, four of those 11 respondents were positive that the EU AI Act would help redress these gaps. Several others flag how we are still in the early stages of the use of AI in the workplace, and that case law and administrative practices have not had time to test the application of regulation. When viewed from this perspective, the scale of regulatory gaps cited amongst our EU-based firms is perhaps less significant than it first appears. Nevertheless, some common challenges still emerge.

Transparency

Obligations and requirements regarding the transparency of automated decision-making is the most cited gap area from the EU-based firms we surveyed. It is also one that feeds into various other gaps referenced, such as the ability to contest an AI decision (i.e. a less transparent decision is harder to challenge).

While most jurisdictions rely on existing data protection rules like the GDPR, our firms in **Poland** and **Sweden** note how these frameworks were not designed with the complexity and opacity of modern AI systems in mind. This is consistent with the fact that the EU's data protection rules were intended to be 'technology agnostic', focused on regulating data rather than any particular underlying technology. As a result, however, respondents flagged how employees can lack the ability to clearly understand algorithmic decisions, particularly in contexts such as recruitment and performance assessment. Our firm in **Greece** characterises this lack of 'explainability' of AI-decision making at work as a key gap.

Our firms in **Denmark** and **Romania** highlight this problem too, focusing on the apparent absence of positive employer obligations in relation to transparency. They note that under existing frameworks there is no clear statutory duty for employers to explain in detail how an algorithm reached a particular decision in recruitment or employment management. Our Irish firm notes the challenges of complying with transparency obligations in respect of the processing of employee personal data under the GDPR when the processing involves AI systems.

Logging and auditability

Our firms in **Denmark** and **Greece** flag the lack of obligations for logging and auditability of AI-driven decisions in current frameworks. Our **Danish** firm, for example, notes that the GDPR does not require employers to maintain detailed records or logs showing how algorithms reach decisions in recruitment or performance management. Our firm in **Greece** highlights the absence of 'auditability' requirements as a key gap in its country's existing framework.

Bias and contestability

Employee protections against bias are also highlighted as a potential gap area. Our firm in the **Czech Republic**, for example, flagged the risk of AI systems replicating flawed and potentially discriminatory decisions when trained on incorrect or biased data. Our firm in **Ireland** further observed that while equality legislation exists, it does not currently impose technical obligations such as ongoing bias testing of recruitment, promotion, or performance algorithms, nor does it require the maintaining of technical logs to support equality-related inquiries which may make it difficult for employers to defend equality claims. These gaps leave room for potential bias to persist unchecked in AI-driven workplace decisions.

Linked with this is the ability to contest bias or problematic decisions made – another key gap cited by our EU-based firms. In **Denmark**, for example, our firm cites evidentiary challenges with the current framework, noting that as the employer or the system provider may not disclose the algorithmic design or training data, employees may face difficulties in substantiating that an AI-driven decision was biased. Our Irish firms' reference to maintaining 'technical logs to support equality inquiries' is also relevant here and goes to the potential issue of employees finding it difficult to challenge automated decisions. Finally, our firm in **Sweden** highlights gaps in liability and accountability, especially when employers use external recruitment platforms. Responsibility remains unclear, and this area is largely untested. They suggest that clearer guidance on this issue will be needed as AI adoption grows.

Contractors

Another gap area cited by several EU respondents is the potential vulnerability of self-employed contractors within existing regulatory frameworks, especially those exposed to algorithmic management via digital platforms. Although the GDPR creates

rights for all natural persons in the EU, such that self-employed contractors are covered by its provisions on automated decision making, they very often fall outside of national employment protection legislation. This challenge is referenced by our firms in **Greece**, **Germany**, **Poland**, **Sweden** and, to a lesser extent, **Denmark**. In **Germany** for example, there are currently few specific protection mechanisms for self-employed persons and hybrid forms of employment. They are not covered by works constitution law, nor do they benefit fully from occupational health and safety obligations or co-determination rights. While this gap might not be inherently caused by the development or deployment of AI in the workplace (rather, it stems from the relevant individuals' employment classification), it remains a significant consideration within the broader regulatory debate on AI and work.

Other 'gap areas'

Other gap areas were also referenced by our firms, albeit less frequently across the survey responses. A particularly interesting one was highlighted by our firms in **Luxembourg** and the **Netherlands** around collective rights. In **Luxembourg**, rules governing employee data processing and the use of automated systems in the workplace apply primarily at a collective level, granting consultation rights to staff representatives rather than individual employees. These rights only apply to businesses that employ a certain number of staff and so individuals in small businesses without representation are effectively excluded from these protections, leaving a notable gap in coverage. This absence of a consultation 'counterbalance' can also increase the risk of legal exposure for employers, as it may foster the (erroneous) perception of an unfettered mandate to explore and adopt technical solutions, leading to more post-implementation employment disputes.

In the **Netherlands**, co-determination provisions grant works councils advisory or consent rights over certain decisions, which could extend to AI deployment in the workplace. However, the provisions that works councils rely on at the moment are "generally worded" and could benefit from some targeted action. One example is to add an item in the list of subjects that would fall under the right of advice or consent that is more specifically linked to the use of AI in the workplace. Such a change would ensure that collective rights remain relevant and responsive to technological developments.

ADDRESSING THESE GAPS AND CHALLENGES

Although not every respondent provided suggestions on how the above gaps could be filled, four of our firms consider that the EU AI Act may assist as it gradually takes effect over the next year or so. Our **Irish** firm provided a particularly useful analysis, noting how the EU AI Act will introduce binding, AI specific obligations and bans that directly address some of the above gaps, especially for employment use cases classed as "high risk". It proposes to mandate the transparency, auditability and oversight needed to protect workers from the risk of AI. As our **Swedish** firm also notes, the EU AI Act introduces mandatory requirements, like transparency, documentation, and human oversight, ensuring that "AI in the workplace is not only ethical by choice but lawful by design".

Non-binding instruments are also expected to play an important role. Our EU-based respondents agree that guidance, voluntary codes, and industry standards can complement legislation by clarifying complex rules, promoting AI literacy, and encouraging best practice. That said, several of our firms also point out that they lack enforcement power and cannot close the gaps identified on their own. Cultural attitudes vary too. In **Denmark**, for example, our firm reports how soft law measures fit naturally within the Danish regulatory tradition, where authorities and the social partners play a central role in developing practical norms through guidance, administrative interpretation, collective bargaining agreements and industry standards. They also note how such instruments provide flexibility and can be updated quickly in response to technological developments, thereby avoiding premature or overly rigid statutory intervention.

Croatia, by contrast, is culturally less receptive to non-binding guidance, favouring clear, enforceable rules - particularly given its already expansive legal framework. Similarly, our firm in **Italy** sees limited scope for soft law/non-binding instruments, citing cultural factors and pointing instead to sectoral collective bargaining agreements as a potential, though slow-moving, solution.

The position in **Germany** should also be noted whereby works councils have a co-determination right on certain issues, such as the implementation of IT systems or rules and conduct in the workplace. Voluntary guidelines do not apply in these areas and so if works councils do not agree with the application of Ministry guidance on the use of AI at work, the employer cannot implement this unilaterally.

As our firm in **Ireland** concludes, the most effective approach to AI regulation will include a mix of legislative provisions and soft measures such as guidance notes, industry standards and training.

Alongside this emerges another theme: the need for more time and practical observation. For example, our **Irish** firm notes that further vulnerabilities in the current regulatory regime may reveal themselves as the EU AI Act is fully rolled out, particularly given the rapid pace of AI development. Similarly, our **Finnish** firm highlights that we are still in the early stages of the AI Act with limited visibility into the full future impacts of AI in the workplace. Elsewhere, our **Croatian** firm observes that in their jurisdiction employers rarely use AI workplace tools and there is no case law yet to identify regulatory gaps.

> *"The main challenge is therefore one of interpretation and implementation, not of legal absence."*
>
> **Elsebeth Aaes-Jørgensen**
> **Partner, Ius Laboris Denmark**

Our firm in **Denmark** echoes this, noting that the effectiveness of existing provisions in covering AI-driven decisions has not yet been tested in case law or administrative practice.

For our firm in **Italy**, a country that has introduced specific AI legislation into its national framework, the main challenge currently lies in the lack of clarity regarding definitions, the scope of application, and the interrelation among the various legislative instruments governing the use of AI in the workplace. This underscores that, for many jurisdictions, including those that might on paper be ahead when it comes to AI regulation, more time might be needed to allow frameworks to evolve and policy makers to better understand the practical application of this rapidly developing technology. It's a familiar story. When the GDPR came into effect, it took some time before enforcement began and norms developed. The EU AI Act may well evolve in the same way.

Our **Danish** firm summarises it nicely as follows: practical application and enforcement will ultimately determine whether protections are sufficient in practice. For this reason, the main challenge is therefore one of interpretation and implementation, not of legal absence.

It could be argued that this need for additional time will only be amplified should the EU AI Act (and GDPR) be amended following the Digital Omnibus proposals.

ELSEWHERE IN EME

THE CURRENT REGULATORY LANDSCAPE

Outside the EU, the other firms we surveyed in the EME region showed a split in regulatory approach. While the UK and Israel are more focused on guidance and non-binding principles, others are moving towards the introduction of AI-specific legislation. In practice though, there is a suggestion that some employers in the region are already converging around EU-style guardrails as a gold standard – evidence perhaps of the 'Brussels effect' being in play.

A more light-touch approach?

In contrast to the EU, several important (non-EU) economies in Europe and the Middle East have not introduced specific AI legislation and, in some cases, tend to rely more heavily on non-binding guidelines alongside existing data privacy and employment law frameworks. This paints a less prescriptive, more 'light-touch' picture for regulating AI in the workplace when compared to the specific binding AI rules in the EU.

In the **UK** for example, our firm reports how non-binding instruments serve as the primary approach to regulating AI in the workplace (and AI more broadly). This aligns with the 'principles-led' focus that the previous UK government opted for in 2023. Although not prescriptive, these principles have a clear conceptual and thematic overlap with many elements of the EU AI Act (and similar emerging legislation globally).

Complementing this guidance is existing legislation. In the **UK**, employment rights legislation is 'technology agnostic'. The UK's key equality legislation for example, treats discrimination against an applicant for a role as discrimination irrespective of whether the cause of that discrimination was attributable to an AI tool or a human decision maker. The focus is on the actions and behaviours of employers, not the technology which facilitates those actions and behaviours.

Furthermore, and to the extent AI is used, the rules under UK data protection law (as will be updated in early 2026 under the Data (Use and Access) Act 2025) provide that wherever a significant decision is made even partly on personal data and based solely on automated processing, the data controller must ensure there are safeguards in place. These safeguards include:

- providing the data subject with information about any decisions;
- enabling them to make representations about them and to contest them; and
- enabling them to obtain human intervention.

In **Israel** too, our firm reports how non-binding ethical principles, voluntary standards, and guidance documents are preferred over rigid legislation. This fits with Israel's policy-led, sector-based approach guided by its AI Policy on Regulation and Ethics that was published in December 2023. This policy document emphasises 'responsible innovation', balancing technological progress with ethical safeguards. The Israeli Data Protection Authority has also issued both official and draft guidelines regarding privacy in the use of AI systems, aiming to strengthen principles such as transparency, accountability, and data security when employing AI tools.

As with the UK, these guidelines are complemented by existing frameworks. Israel's Protection of Privacy Law, as amended in August 2025, for example, applies to AI systems processing personal data, requiring privacy-by-design, transparency, and lawful processing. Obligations under Israeli employment law frameworks also apply to the use of AI in the workplace.

Finally, **Türkiye** has not yet established specific regulations governing the use of AI systems in the workplace; however, there are general rules and guidance documents that directly affect such practices. The 'Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence' published by the Turkish Personal Data Protection Authority are central in this regard. Employees are then also covered by general labour law, with the rules also applicable when AI tools are used for hiring or performance management. Under the existing data protection framework, individuals have the right to object to the processing of their personal data through automated means and to request information on how and by whom their data are processed, which provides a certain level of transparency when it comes to the use of AI at work.

Specific AI regulation is on the horizon

In contrast to these trends, the other two respondents that we surveyed in the EME region, our firms in **Switzerland** and **Kazakhstan**, confirm that dedicated AI frameworks are either here or on the horizon.

For **Switzerland**, the Federal Council has tasked the administration with drafting an AI bill by the end of 2026 to implement the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights. The Swiss Bill is expected to set out measures on transparency, data protection, non-discrimination and supervision, with an accompanying plan for non-binding industry solutions in the same timeframe.

On 17 November 2025, **Kazakhstan** adopted a law on artificial intelligence, which entered into force on 18 January 2026, laying down high-level principles and specific curbs (including bans on emotion recognition without consent and real-time facial recognition in public spaces), with sectoral rules to follow. This includes anticipated Labour Code amendments and the introduction of a National AI Platform to be overseen by a future Ministry of AI.

There may also be developments on the horizon for the **UK**. The current government has signalled plans for "appropriate legislation" to place requirements on developers of highly capable AI models. While no draft has been published yet, reports suggest an AI Bill could emerge after May 2026, likely narrowly focused on safety and accountability rather than sweeping workplace rules. Separately, broader proposals such as the House of Lords Private Members' Bill and the Trade Union Congress draft "Artificial Intelligence (Regulation and Employment Rights) Bill" have been floated, but both have failed to gain traction and are unlikely to materially influence the UK approach.

IS THE CURRENT LANDSCAPE ADEQUATE?

Three of the five firms surveyed identified potential gap areas in their countries' current landscape. The 'main gap' identified by our firm in **Israel** is the absence of an explicit statutory obligation for employers to disclose the use of AI in recruitment or management. Our firm in **Kazakhstan** notes how existing employment and data protection laws do not clearly define what safeguards employers must provide when using AI for surveillance or recruitment, nor who is responsible when AI makes an error. Finally, our firm in **Türkiye** notes how self-employed and platform workers fall outside the scope of the Labour Law and are therefore particularly vulnerable to some of the risks associated with the use of AI.

Elsewhere, our firm in **Switzerland** notes that while existing employment rights legislation does not leave any specific regulatory gaps, challenges arise from the fact that AI systems are subject to different legal requirements across various regulatory areas. Each provision relies on its own terminology; for example, the concept of a "behavioural monitoring or control system" in workplace health and safety law, or "automated individual decision-making" and "high-risk profiling" under data protection law.

ADDRESSING THESE GAPS AND CHALLENGES

As regulators grapple with how best to manage AI risks in the workplace, responses across the region reveal strikingly different strategies, from legislative action to reliance on guidance and internal governance, set against the backdrop of global influences such as the 'Brussels effect'.

Our firms in **Switzerland**, **Kazakhstan** and **Türkiye** all reference potential legislative solutions to address the above limitations in their countries' current frameworks. In **Switzerland**, for example, the above challenges relating to fragmentation are expected to be addressed as part of the broader development of a general legal framework planned to be drafted by the end of 2026. The drafting process will be followed by the standard legislative process, including a consultation procedure and deliberations in Parliament. At present, it remains unclear when the entry into force of the general legal framework is planned or will actually occur. Our firm in **Türkiye** reports how new AI-specific legislation would help close the gaps for non-standard workers (i.e. contractors). Similarly, our firm in **Kazakhstan** suggests that the adoption of AI-specific legislation remains necessary to ensure consistent protection of workers' rights, establish clear liability rules, and guarantee legal certainty for both employers and employees.

A slightly different view is expressed in the **UK**, where current and new guidance is expected to remain the 'main' or 'primary' method through which the jurisdiction will regulate the use of AI in the workplace, offering a collaborative approach to building the regulatory picture. For example, the UK data protection authority's recent report on agentic AI is designed to allow organisations to understand their "early-stage thinking on speculative opportunities and risks".[7] Rather than the data protection authority regulating in a vacuum, this offers stakeholders the opportunity to contribute to the regulatory thinking as the data protection authority prepare their statutory code of practice on AI and automated decision-making which is intended to provide "clear and practical guidance on transparency and explainability, bias and discrimination and rights and redress, so organisations have certainty on how to deploy AI in ways that uphold people's rights and build public confidence".[8] Our UK firm further suggests that any legislation on AI is likely to be targeted and narrow, intended to resolve particular issues, rather than regulate in any general sense. To this end, the implementation of a suite of new related rules to address AI in the workplace is not currently expected in the UK.

Finally, our firm in **Israel**, a country which also adopts a strategy primarily focused on non-statutory measures to address AI-related risks, considers 'self-regulation' to be the most effective way to deal with risk areas, alongside existing obligations. This requires both clear policies and guidance as well as training for managers and employees. **Kazakhstan** also recognises the importance of internal governance to regulate the use of AI, noting how internal measures can play an important transitional role by helping employers create preliminary safeguards and accountability mechanisms until national legislation catches up with technological developments.

The 'Brussels effect'

Against this backdrop of varied approaches and transitional measures, another dynamic comes into play - the influence of the 'Brussels effect' on AI regulation.

As noted above, the 'Brussels effect' describes the EU's ability to set global standards as companies adopt its rules worldwide to maintain market access. Many organisations would like to adopt jurisdiction-agnostic AI compliance and governance as far as possible – seeking to follow a gold-standard that avoids the need to adopt, say, 20 different country-specific regulatory structures. This has long been the case in respect of data protection, and our UK firm expects a similar trend to emerge with the EU AI Act.

Why does this matter? While there may be some temptation from the non-EU countries in the EME region, and indeed other regions, to converge with the EU's approach, our UK firm identifies a potential, opposing trend. They note that (to some extent) the 'Brussels effect' may apply in respect of the EU AI Act such that organisations will adopt its key principles as part of internal policy documentation. As a result, certain non-EU countries may not see any urgent need to layer further or differing prescriptive regulation on top of this.

THE AMERICAS

The Americas are moving toward greater regulation of AI in the workplace, but seemingly along different paths.

Peru, Mexico, Colombia, and **Chile** appear to be aligning with the EU's risk-based legislative approach, introducing (or proposing to introduce) frameworks that classify certain workplace AI systems as high-risk and that, in some cases, establish transparency and human oversight obligations. By contrast, the **US** regulatory landscape remains fragmented, driven by state and local laws focused on workplace AI, despite federal ambitions for a unified national standard.

Despite these nuances, common gaps emerge across the region regarding current regulatory frameworks. These include challenges regarding transparency, contestability, bias mitigation, and enforcement capacity - even where specific AI laws exist.

Peru's experience offers a cautionary lesson: passing legislation is not always enough to address these gaps. Without strong enforcement capacity and institutional readiness, even well-designed rules risk remaining aspirational. Non-binding measures such as internal governance and training are also seen as valuable ways of addressing potential inadequacies in existing frameworks.

THE CURRENT REGULATORY LANDSCAPE

If the EU wins out as having the most countries in our survey with specific AI legislation, the Americas follows in second place. In several cases, this legislation is heavily inspired by the risk-based approach adopted under the EU AI Act.

The introduction of specific AI regulation is certainly accelerating in the region with draft legislation proposed in **Chile**, **Colombia** and **Mexico**. Meanwhile, **Peru** and the **US** stand out in our wider survey as the only two countries outside of the EU that have introduced specific AI legislation. In the **US**, this regulation is positioned at a state and local level, rather than at the federal level, in spite of the current US administration's competing desire to enact a national, centralised pro-AI framework.

Alongside this regional theme of specific AI regulation, existing frameworks play a part too, as reported by our firms in **Mexico** and **Colombia**. **Colombia** has also introduced non-binding guidance which aims to promote the responsible and transparent use of AI, human oversight, and respect for fundamental rights.

Specific AI legislation: A convergence with international trends

When examining specific AI legislation in the Americas region, a clear theme emerges of convergence with international trends. Several of the legislative proposals, for example, include similar concepts and provisions to those found in the EU AI Act.

In **Chile**, a Bill to regulate AI proposes a risk-based approach and aims to promote the ethical and sustainable development and implementation of AI in the service of people, safeguarding fundamental rights, democratic principles, and the rule of law. Although the Bill doesn't contain many specific rules regarding the use of AI in the workplace, systems that assess a person's emotional state are included within the category of unacceptable risk systems. Enforcement will sit with the Data Protection Agency, supported by a new Technical Advisory Council on Artificial Intelligence.

Colombia is moving in a similar direction. A draft Bill introduces principles of transparency, accountability, and human-oversight. The Bill proposes the creation of a National Authority for Artificial Intelligence, to be led by the Ministry of Science, Technology and Innovation. If enacted, this authority would be responsible for guiding the implementation of the law, coordinating AI governance, and issuing binding technical opinions on risk-related matters.

> *"From a cross-border perspective, Mexico's approach is converging with international trends: AI systems that affect access to work, employment conditions or human dignity are considered high risk, and regulation is moving toward transparency, accountability and non-discrimination as core principles."*
>
> **Renata Buerón**
> **Associate, Ius Laboris Mexico**

Several initiatives currently under discussion in **Mexico's** Congress also aim to create a clear regulatory framework for AI. One of these, the Federal Law to Regulate Artificial Intelligence, currently under discussion in the Senate, is inspired by the risk-based model found in the EU. High-risk systems include the likes of recruitment and performance evaluation tools, workplace surveillance tools and systems that determine access to employment or training. Under the proposal, use of a high-risk AI tool would give rise to obligations around documentation, transparency, risk assessments and human oversight. Another proposal, in the Lower House, is aligned with Mexico's broader digital transformation agenda and would create a specialised AI supervisory authority.

While the above proposals remain pending, in 2023 **Peru** became the first country in Latin America to adopt a general legislative framework on AI. The Regulation of Law 31814, issued on 9 September 2025, introduces specific and gradual obligations for entities that use AI systems, although many of these have not yet entered into force and are subject to various implementation timelines. The Regulation establishes the technical and legal framework for the development, implementation, and use of AI systems in the country. On the use of AI in the workplace, as with the other frameworks explored above, it classifies the use of AI to determine recruitment, evaluation, hiring, and termination processes of workers or job applicants, as well as setting working conditions as high-risk.

A state-by-state patchwork in the US

The above examples of AI regulation in the Americas, both proposed and in force, are generally standalone frameworks that apply broadly across each jurisdiction and address AI in a wide context rather than focusing solely on workplace use. In contrast, our firm in the **US** reports how regulation there is emerging primarily at the state and local level with a sharp focus on workplace applications.

Various states, including, to date, California, Colorado, Illinois, and Texas specifically regulate the use of AI in the workplace in various ways. This may include, depending on the jurisdiction, notice to employees and the right to opt out of certain processing depending on the use case. California's law further prohibits the use of an AI tool in a manner that discriminates against an applicant or employee. Numerous other states have proposed laws that would similarly impact the use of AI in the workplace, such as New York and Connecticut.

In addition, we also see legislation at the local level. For example, a New York City law restricts employers from using an automated employment decision-making tool in New York City unless a bias audit has been done and notice of the job qualifications or characteristics the tool will assess is provided prior to the tool's use.

In this sense then, the US regulatory landscape remains fragmented, with state-by-state rules shaping the current direction of travel. However, this patchwork approach contrasts sharply with the administration's push for a unified framework. Most recently, the Executive Order signed on 11 December 2025 and entitled 'Ensuring a National Policy Framework for Artificial Intelligence', signals a desire for a single, minimally burdensome national standard rather than several state ones. Whether this ambition will lead to a 'Washington effect' to rival the 'Brussels effect' remains to be seen (some already think it has, as explored in the EU section above), but the tension between national and local regulation is clear.

Nevertheless, and in the absence of federal legislation, our US firm suggests that for now employers can expect the legal landscape to continue to develop as a patchwork of state and local laws. They will need to evaluate AI requirements on a state-by-state basis before implementing an AI tool that processes employee or applicant data or otherwise impacts the terms and conditions of employment.

Beyond 'general' frameworks'

The **US** is not the only country in the region with regulation directly targeting the use of AI at work. A unique feature of **Colombia's** draft regulation, when compared to others explored in this publication, is its acknowledgment that AI will transform job functions and labour relations. The proposed regulation therefore:

- Promotes a fair transition to ensure workers can adapt to technological change through retraining and re-skilling;
- Requires the State and employers to implement training and capacity-building programmes in digital and AI competencies, particularly for vulnerable populations and regions;
- Mandates that the adoption of AI in the workplace must respect fundamental labour rights, including dignity, non-discrimination, job stability, and collective participation; and
- Encourages social dialogue and cooperation between government, employers, workers, and the education sector to anticipate the impact of AI on employment and promote human talent development.

This focus on anticipating and managing the industrial impacts of AI, particularly on employment and workforce dynamics, makes Colombia's draft regulation noteworthy, as it goes beyond technical governance to address broader socio-economic transformation.

IS THE CURRENT LANDSCAPE ADEQUATE?

Four of the five firms we surveyed in the region identified potential gaps with their existing frameworks, although as with the EU firms we surveyed, there was a mixed response as to the extent of these gaps.

At one end, our firm in **Mexico** notes how existing rules regarding data protection and labour law already offer 'real safeguards'. On the other, our firm in **Peru**, a country that has specific AI legislation in place, reports that 'to almost no extent' does the existing regulatory framework adequately protect workers when employers use AI or algorithmic management tools. In any event, some common gaps emerge from the responses, several of which relate to issues around transparency, contestability and bias.

In **Mexico**, for example, our firm notes that there is currently no positive duty for employers to provide explanations of model logic or data sources, an issue linked to the transparency of automated decision making, but which then also makes contesting a decision difficult in practice. Our firm also notes that there are currently no detailed rules on how automated decisions should be documented, audited or explained, especially for high-risk AI uses such as in: hiring, shift allocation, productivity monitoring, or dismissal. Meanwhile, our firm in **Colombia** suggest that existing frameworks do not explicitly address automated decision-making, algorithmic transparency, or bias mitigation.

Concerns in **Peru** also span these commonly cited gap areas, but importantly, these are said to persist despite the recent introduction of specific AI legislation. While the gradual implementation of the relevant regulation is seen as being partly to blame here (i.e. many of the provisions remain aspirational rather than enforceable at this stage), our firm also notes that the framework fails to guarantee enhanced explanations of automated decisions, meaningful human review, limits on automated decision-making, or safeguards against discriminatory outcomes. There are also concerns that an absence of clear sanctions for improper or non-transparent use of AI will reduce the effectiveness of the legislation, and that the above issues will disproportionately impact workers outside of standard employment relationships (i.e. self-employed contractors).

In the **US**, the nature of AI tools, including their complex development and training, is cited as a key reason why legislatures have deemed it necessary to pass AI-focused legislation, particularly to ensure that the tools are trained to and continue to function in a non-discriminatory manner. That is notwithstanding the fact that existing laws provide protection against intentional discrimination by any means, including through technology like AI.

Other potential gaps also emerge in the region, particularly around enforcement. In **Mexico**, for example, our firm reports how enforcement is fragmented across labour authorities, data protection regulators and sector-specific bodies, with no single supervisor dedicated to algorithmic management. Elsewhere in **Peru**, whilst the new AI regulation designates as high-risk the use of AI systems for recruitment, evaluation, hiring, termination, and the determination of working conditions, our firm suggests that it does not specify how authorities will detect such use, evaluate compliance, or impose corrective measures. Added to this is the technical complexity of many AI systems, which makes it difficult to determine when and how an employer is using AI. As a consequence, in practical terms, supervisory authorities face serious limitations in identifying and monitoring the use of AI. Our Peruvian firm therefore has concerns that, without effective transparency and detection mechanisms, the enforcement of AI-related obligations will be highly challenging.

ADDRESSING THESE GAPS

The region offers useful policy lessons on how to close these gaps, particularly around the role of legislation and what is required for this to be effective.

In **Mexico**, our firm notes how the current law protects workers, but at the same time, the rules do not yet form a coherent framework for AI in the workplace. Importantly, the several proposals in Congress recognise these issues and aim to create a clearer framework, introducing risk-based rules for AI systems used in workplaces, registration and oversight of high-risk tools, such as those used in hiring or performance management, audits and human review, and a specialised supervisory authority. While new legislation is therefore not viewed as essential, our firm suggests that it would help close transparency gaps, strengthen accountability and make it easier for people to understand and challenge decisions that affect their working lives.

Our firm in **Colombia** take a similar view. They report that the current framework still requires binding regulation - such as the pending draft Bill - which can establish clear obligations, oversight mechanisms, and workers' rights specific to AI-driven management and decision-making.

However, **Peru's** experience underscores that legislation alone is not enough. As our Peruvian firm reports, binding rules must be paired with robust mechanisms for supervision, monitoring, and enforcement. At present, Peru is seen to lack the infrastructure, technical capabilities, and institutional mechanisms needed to effectively oversee AI use in the workplace. Without these, even well-designed laws risk remaining aspirational rather than practical.

As with the EU, across the Americas, non-binding instruments are also expected to play a part alongside legislation. For example, both our firms in **Mexico** and **Chile** highlight guidance, voluntary codes, and training as important complements to legislation. Our **Chilean** firm particularly stresses that internal company procedures and worker training are essential to ensure ethical AI use and to protect personal data and fundamental rights - legislation alone cannot achieve this.

Against this, our firm in **Colombia** warns that soft law cannot guarantee remedies for discrimination or unfair dismissal, although it echoes its importance for raising organisational awareness. In a similar vein, our **Peruvian** firm highlights the limits of voluntary measures, noting

that without enforcement, compliance is unlikely. In the **US** too, our firm suggests that without specific legislative and regulatory guardrails, it may be unrealistic to expect a consistent reaction from private employers to such voluntary measures. Certainly, the proliferation of actual legislation, and anticipated future legislation, suggests that mere voluntary guidance will not be used in lieu of regulation in the US.

In terms of where we land then, our **Mexican** firm concludes that non-binding measures are a helpful and realistic starting point. They can be launched quickly, give clarity to employers, and help protect workers in the short term. But they are not a substitute for binding rules in areas where decisions made by algorithms can affect people's dignity or access to work. As a result, they suggest that a combined approach is likely: guidance and standards now, paired with targeted legislation for the high-risk uses of AI in the workplace.

Yet, whether said regulation is targeted or general, **Peru's** experience serves as a cautionary reminder that legislation alone is not enough. Without strong enforcement capacity and institutional readiness, even well-designed rules risk remaining aspirational. For the region, this underscores that effective governance requires not only clear laws but also robust oversight mechanisms and complementary non-binding measures, including internal governance.

> *"A combined approach is likely: guidance and standards now, paired with targeted legislation for the high-risk uses of AI in the workplace."*
>
> **Renata Buerón**
> **Associate, Ius Laboris Mexico**

ASIA-PACIFIC

The APAC jurisdictions we surveyed currently rely on existing employment and data protection laws, supplemented by non-binding guidance and ethical frameworks, rather than prescriptive AI-specific legislation. This hybrid approach reflects a preference for flexibility and proportionality, though it is worth noting that some jurisdictions, such as China, which has introduced several AI regulations, and South Korea, which recently implemented its AI Basic Act, could be moving toward more comprehensive frameworks. Meanwhile, recent legislative developments in **Australia** signal a move towards greater oversight of automated systems. Additional, targeted measures, together with increased union involvement, could also be on the horizon.

Non-binding instruments carry significant weight in the APAC region, with guidance increasingly regarded as practical compliance benchmarks for employers.

Common gaps are identified and include the absence of statutory rights to explanation or human review of automated decisions, limited requirements for algorithmic impact assessments, and unclear liability for AI-mediated decisions.

To address these gaps, some firms in the region point to targeted enhancements to existing laws combined with governance frameworks, rather than comprehensive AI-specific employment legislation, to balance innovation with worker protection. Our firm in Australia considers this to be a real possibility, given the current direction of travel.

THE CURRENT REGULATORY LANDSCAPE

None of the firms based in the APAC region that we surveyed have a specific AI regulation in place. Instead, regulation is centred on existing laws, supplemented by non-binding frameworks and regulator guidance. In fact, when compared to the other regions, the countries that we surveyed in the APAC region stand out as giving the greatest weight to non-binding instruments. These work in tandem with existing employment and data protection frameworks.

While **Australia** broadly mirrors this regional trend, currently relying on existing frameworks and non-binding guidance, it also presents some nuances. The regulatory landscape is evolving quickly, with unions calling for stronger safeguards and the government signalling targeted reforms. We also see a growing union influence in practice, with new 'AI Implementation Agreements'. In this section, we examine:

1. The common regulatory position across **Hong Kong, Singapore, New Zealand** and **Malaysia**; and
2. **Australia's** broadly similar position, alongside the jurisdiction-specific nuances that distinguish it from the other surveyed countries.

Existing frameworks and non-binding guidance

In **Hong Kong**, our firm notes that the current approach is best described as context and risk-based. Existing legal regimes apply to AI-enabled activities, and regulators influence responsible adoption through non-binding guidance that is becoming a practical compliance baseline for employers.

The principal statutory regime is the Personal Data (Privacy) Ordinance ('PDPO'), which applies whenever personal data is collected, used or otherwise processed in connection with AI systems. Anti-discrimination legislation also applies, alongside sector-specific guidance for regulated industries.

For employers, the Office of the Privacy Commissioner for Personal Data ('PCPD') has issued non-binding guidance relevant to workplace AI. In particular:

- The PCPD's checklist on the use of generative AI by employees sets expectations for internal governance, privacy compliance, human oversight and bias mitigation when employees use generative AI tools.
- The PCPD's 'Artificial Intelligence: Model Personal Data Protection Framework' recommends that organisations adopt an AI strategy and governance structure (for example, an AI governance committee), conduct comprehensive risk assessments (including privacy impact assessments) and implement measures to ensure ongoing PDPO compliance when preparing, training or deploying AI systems.

Separately, the Hong Kong Government issued an Ethical AI Framework in July 2024 for use across government, which also serves as a non-binding reference for the wider

> *"These materials are not legally binding, but they are increasingly regarded as baseline expectations of responsible AI deployment […]."*
>
> **Gladys Ching**
> **Managing Associate,**
> **Ius Laboris Hong Kong**

community regarding principles, good practice and assessment templates for AI and big data analytics.

Similarly, in **Singapore**, our firm notes how the approach currently adopted is sectoral, risk-based and outcome-oriented, anchored in existing laws, while supplemented by non-binding frameworks and regulator guidance. In fact, our firm describes non-binding measures as being “central to Singapore’s AI governance model.”

The Personal Data Protection Act 2012 (‘PDPA’) provides the core statutory obligations applicable to the AI-enabled processing of employees’ personal data, including requirements around notification of purposes, consent (and limited statutory exceptions), purpose limitation, accuracy, protection, retention, access/correction rights, data breach notification, and accountability. Employers deploying AI systems, such as algorithmic screening, productivity monitoring tools, or biometrics, must comply with these PDPA obligations and demonstrate appropriate governance, including risk assessments, policies, training, and vendor management.

Beyond the PDPA, the Ministry of Manpower and the Tripartite Alliance for Fair and Progressive Employment Practices administer the Tripartite Guidelines on Fair Employment Practices and the Fair Consideration Framework, which apply to hiring and workplace practices regardless of whether AI tools are used. These frameworks prohibit discriminatory practices and require fair, merit-based selection. Singapore is also progressing Workplace Fairness Legislation, which is expected to codify prohibitions against discrimination in key protected areas and introduce clearer redress mechanisms; AI enabled practices in recruitment and employment will need to comply with these statutory standards once in force.

Regulatory guidance specific to AI is largely non-binding but regarded as ‘influential’

by our Singaporean firm. The Personal Data Protection Commission ('PDPC') and the Infocomm Media Development Authority have issued the 'Model AI Governance Framework', the 'Implementation and Self-Assessment Guide for Organisations', and the 'AI Verify testing framework and Foundation', which set out practical governance measures for transparency, explainability, human oversight, robustness, and accountability. Sector regulators have published complementary guidance for AI uses within their areas.

Collectively, our Singapore firm reports how this ecosystem regulates AI in the workplace through enforceable data protection and employment laws, augmented by widely-adopted governance frameworks rather than prescriptive technology-specific rules.
In **Malaysia**, non-binding instruments also play a key part in the regulatory landscape. In particular, the government has published the 'National Guidelines on AI Governance and Ethics', which are intended as voluntary guidance for industry players whilst the Government develops laws to regulate the use of AI. The Guidelines suggest that: (i) when using AI in the workplace employees should be notified of such use; (ii) employees' privacy should be respected, as required by law; (iii) the use of AI in the workplace should be consistent with HR policies; and (iv) employers should ensure AI are free from bias.

The Personal Data Protection Commissioner in Malaysia is also developing specific guidelines for the use of automated decision-making in processing personal data. Once specific guidelines for automated decision-making have been developed, these are expected to further influence how employers can use AI in the workplace.

Finally, in **New Zealand**, our firm reports how, rather than introducing a standalone 'AI Act', the Government has taken a light-touch, risk-based self-regulatory approach, relying on existing employment law obligations and frameworks, voluntary guidelines, technical standards, industry-led codes of practice, and oversight by the Privacy Commissioner. For example, the Government has issued the Algorithm Charter for Aotearoa New Zealand, which commits signatories to principles of transparency and fairness, and ensuring that New Zealanders can have confidence in how government agencies use algorithms. Additionally, the Public Service AI Framework provides guidance to support the responsible development and deployment of AI across public sector agencies.

When viewed through the lens of these four major economies in the region, AI governance in the APAC region appears to be characterised by a hybrid approach: enforceable obligations under existing data protection and employment laws, complemented by voluntary frameworks and regulator-issued guidance that increasingly set practical compliance benchmarks - comparable to the approach adopted in the **UK**. These non-binding instruments, together with industry-led standards and ethical principles, are shaping workplace practices as the technology evolves.

Competing perspectives emerge in Australia

It’s a similar story in **Australia**, which broadly follows the above regional trends, although regional nuances emerge.

As with the other APAC countries surveyed, for example, our Australian firm notes how existing workplace laws already apply in the context of the use of AI and automated decision making in the workplace. Unfair dismissal laws, anti-discrimination statutes, adverse action provisions and work health and safety legislation all play a role in safeguarding employees.

Consultation requirements are another area of focus. Most employees in Australia are covered by modern awards or enterprise agreements that mandate consultation when major changes, such as the introduction of new technology, are likely to have a significant effect on employees. These obligations are broad enough to encompass AI and automated decision making, ensuring that employees and their representatives are involved in discussions about technological change.

Complementing this landscape, albeit to a lesser extent than with other surveyed countries in the region, are non-binding guidelines. This includes, for example, the ‘Guidance for AI Adoption: Foundations’ published by the Department of Industry, Science and Resources.

Like the other APAC jurisdictions we surveyed, there are also no plans to introduce a dedicated AI Act following the publication of the Government’s National AI Plan on 2 December 2025.

Despite all this, and while the Australian Government appears to be moving away from a ‘dedicated AI Act’, recent developments signal a move towards greater oversight of automated systems. For example, and as at the time of publication, proposed amendments to the Workers Compensation Act 1987 (New South Wales) aim to ensure human oversight in key decisions, prevent unreasonable performance metrics and surveillance, and grant unions increased powers. These amendments may provide a blueprint for similar laws in other jurisdictions and could therefore be indicative of more targeted legislative amendments to come.

In fact, while employer representatives are heralding the supposed “light-touch” approach in the National AI Plan that signals a retreat from the introduction of a comprehensive AI framework, the rhetoric from the Government suggests there is still an appetite for union-backed reforms to the Australian framework. These proposals include a right for workers to refuse to use AI in certain circumstances, mandated training, reforms to surveillance laws, and expanded bargaining rights related to AI adoption.

While these reforms are still in their early stages, the use of mandatory "AI Implementation Agreements" has also emerged as a more concrete example of increasing union involvement and influence in Australia's AI landscape. At the Federal level, unions, led by the Australian Council of Trade Unions ('ACTU'), are advocating for these agreements, that would require employers to consult with staff before introducing new AI technologies. They would guarantee job security, skills development, retraining, and transparency over technology use. Most recently, we saw Microsoft Australia and the ACTU announce an agreement to "develop a framework to elevate the voices and expertise of working people in the introduction of AI and other emerging technologies into Australian workplaces". The agreement, which is a first in Australia, is grounded in three core objectives: information sharing with union leaders and workers, worker voice in technology development, and collaboration on public policy and skills.

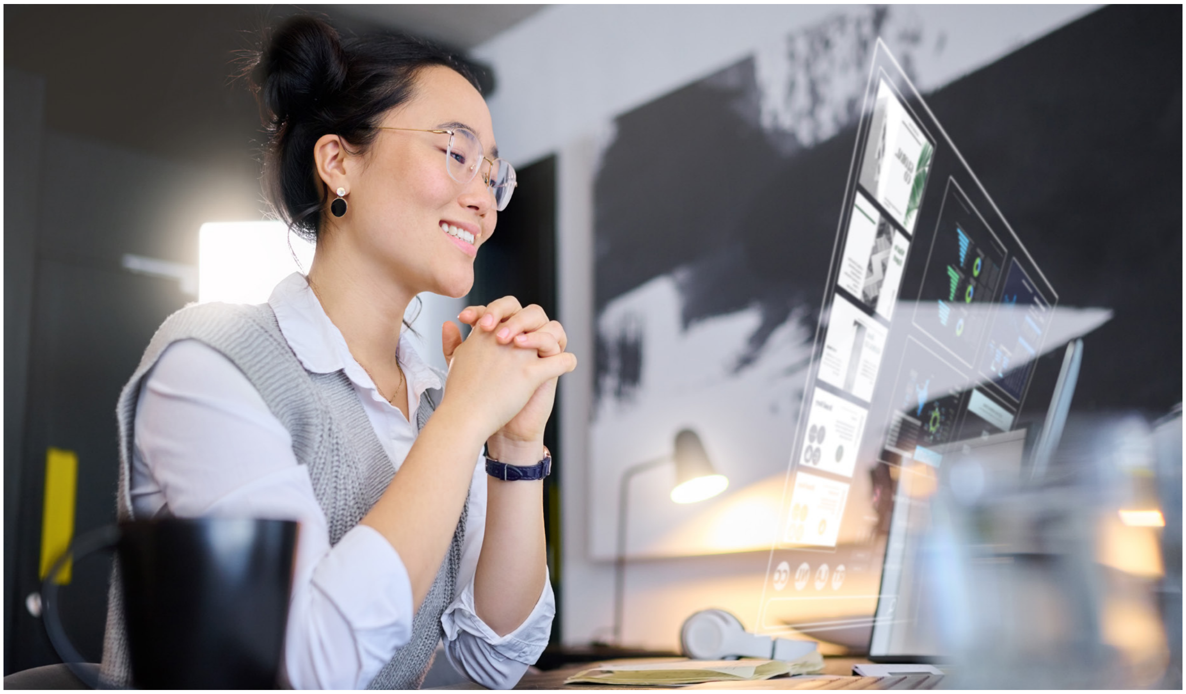
While a comprehensive, EU-style AI Act appears unlikely in Australia, the combination of emerging legislative proposals and expanding union influence suggests that employers should be prepared for more targeted legislative changes which give workers and unions greater voice in the adoption of AI in the workplace.

IS THE CURRENT LANDSCAPE ADEQUATE?

As with other countries surveyed, there is a sense from the firms we surveyed in the APAC region that existing frameworks provide a reasonable level of protection for employees. Even so, key gaps are identifiable.

Our firm in **Singapore**, for example, notes that existing employment and data protection laws are said to provide "meaningful protections" for employees against harmful AI uses, but "coverage is uneven and there are identifiable gaps."

Employment protections stem from the Employment Act and Tripartite Guidelines, which require fair, merit-based practices regardless of whether decisions involve AI.



The PDPA provides strong safeguards for personal data used in AI systems, including transparency, purpose limitation, and breach notification. Employers must assess proportionality and implement safeguards when deploying high-risk AI.

Despite these frameworks, several gaps and limitations are identified. First, there is no statutory right to an explanation of automated decisions or a mandated human review of decisions with significant effects, unlike in certain other regimes. While PDPC guidance encourages explainability, human oversight, and contestability, these are not codified obligations. Second, discrimination controls are currently enforced through guidelines and licensing/administrative levers; the forthcoming Workplace Fairness Act is expected to strengthen these protections, but until enacted, redress mechanisms rely on existing administrative processes. Third, there is no legal requirement to conduct algorithmic impact assessments, though accountability principles and PDPC guidance recommend risk assessments, testing and monitoring, especially for high risk uses. Fourth, workplace surveillance and productivity monitoring via AI raise proportionate use questions. Exceptions under the PDPA, such as legitimate interests and deemed consent by notification, require careful application but may not fully address expectations of fairness and dignity at work.

Meanwhile, in **Hong Kong**, our firm describes a similar picture; one where the existing frameworks are somewhat robust, but not watertight when it comes to AI at work.

Employee rights are primarily governed by the Employment Ordinance, which applies regardless of whether AI tools are used. Employers must uphold duties of care and mutual trust when deploying AI. Anti-discrimination laws - including the Sex, Disability, Family Status, and Race Discrimination Ordinances - prohibit bias and harassment in employment decisions, including those assisted by AI. These protections extend to a wide range of workplace participants, and employers may be vicariously liable for unlawful acts unless they take reasonably practicable steps to prevent them.

Again, and despite what appears to be a meaningful level of protection provided by the existing framework, gaps are identified. From a data privacy perspective, transparency, impact assessments and contestability for high-risk automated decisions are all seen as absent from the current regulations. From an anti-discrimination perspective, clearer liability for AI mediated decisions and calibrated obligations on vendors are identified as being required.

In **New Zealand**, our firm also note how existing obligations relating to employment, including non-discrimination and privacy, continue to apply and provide protections when employers use AI or algorithmic management tools. In particular, they report how the indirect discrimination provision in the Human Rights Act offers a broad mechanism: a practice, such as an algorithm, that has the effect of disadvantaging a person or group on one of the prohibited grounds is unlawful unless there is a "good reason" for it. Additionally, under the Privacy Act, the use of personal information in AI tools must be carefully managed, as inputting personal data about an individual can give rise to privacy breaches.

Even so, there is a recognition that AI introduces considerations that were not explicitly contemplated when these laws were drafted and as such, there may be areas that are not as adequately dealt with by the current frameworks.

Similarly, our **Australian** firm notes how existing workplace laws already provide a "foundation of protections" relevant to the use of AI and automated decision making in the workplace. For example, it is noted that even if an algorithm makes a decision to terminate employment without human oversight, the employer remains liable under unfair dismissal laws. The Fair Work Commission would still require a valid reason for dismissal and would assess whether the process was fair and reasonable. Although more nuanced, discrimination law is also seen as capable of capturing circumstances where a prospective employee has been rejected for discriminatory reasons, regardless of whether a human or an algorithm made the decision.

In terms of potential gaps, our Australian firm does not identify any significant issues with the current regulatory framework, although they recognise that some existing laws may be in need of modernisation to keep pace with technological change. It is a different story on the ground, however. For example, recent committee reports and union submissions argue that the consultation duties referenced above are sometimes "obviated by employers" and may lack transparency in practice, creating uncertainty over whether AI deployment constitutes a major change triggering formal consultation. Our Australian firm further notes that while there is little proof that this is the case, this argument is quickly gaining support in the Federal Cabinet. This goes to the wider theme in Australia explored above of increasing union influence in workplace AI regulation and potential targeted changes to Australia's legislative framework.

Finally, **Malaysia** is slightly less confident when it comes to the current regulatory framework, noting how the protections are inadequate, since existing employment laws and regulations do not contain specific protections for employees when employers use AI. Potential issues include employees being subject to decisions concerning their employment which were made solely by AI, and the use of AI to monitor or track employee behaviour.

ADDRESSING THESE GAPS

Our firms in both **Singapore** and **Hong Kong** suggest that comprehensive, standalone AI-specific employment legislation is not necessary to fill these gaps. Instead, they both report how strengthening and clarifying existing frameworks through targeted statutory measures, combined with guidance and other non-binding instruments better aligns with the regulatory philosophies of each jurisdiction.

For **Hong Kong** this hybrid approach would align with its incremental, risk-based policy approach while materially strengthening individual protections. For **Singapore**, it aligns with its regulatory philosophy and provides practical, proportionate protection without unduly constraining innovation in the workplace.

Elsewhere, our firm in **New Zealand** focus on the internal governance of AI use at work. They note how workplace policies in particular play an important role. Developing and implementing an AI policy helps ensure transparency around its use in the workplace and sets clear expectations for responsible and accountable conduct by both employers and employees.

Where employers are considering using AI in the recruitment process, they are encouraged to first seek specific legal advice around the intended use of AI and how it can be communicated to candidates.

Our firm in **Malaysia** also sees the value of non-binding instruments and hopes that the specific guidelines on automated decision making that are being developed may help fill some of the gaps noted above. In fact, they consider the use of non-binding measures such as guidelines and best practice frameworks to be the balanced position, as they allow regulators to quickly amend these documents to address recent technological developments without going through lengthy legislative processes. Even so, without any specific mandatory requirements/ prohibitions, our firm notes that there will always be gaps in protection for employees, contractors, and other workers.

In this sense then, and perhaps more so than in other regions, the value of non-binding instruments as a regulatory tool is emphasised, even if this still needs to be complemented by specific and targeted legislative solutions.

Interestingly in **Australia**, targeted legislative amendments could become a reality sooner rather than later. As our Australian firms notes, while existing laws offer protections, the regulatory landscape is evolving quickly, with unions calling for stronger safeguards and the government signalling targeted reforms.

> *"This hybrid approach [...] provides practical, proportionate protection without unduly constraining innovation in the workplace."*
>
> **Lionel Tan**
> **Partner, Ius Laboris Singapore**

Having examined the key stats behind the scale and pace of AI adoption and then mapped the regulatory landscape by region, we now seek insights from some of our experts. In the following interviews, specialist data-protection lawyers from the UK, Mexico and Singapore share their perspectives on workplace AI regulation in their region and how these fit within the global picture. They also provide key practical pointers, essential for employers when it comes to the use of AI at work.

03

IN CONVERSATION WITH OUR EXPERTS: PRACTICAL PERSPECTIVES ON WORKPLACE AI

ALEXANDER MILNER-SMITH

Co-Head of Ius Laboris UK's Data, Privacy & Cyber Group and Chair of the Ius Laboris Data Privacy Expert Group

How would you sum up the current landscape for workplace AI regulation in the region?

The EME landscape already offers substantial worker protections through a dense mix of binding law and soft guidance - anchored by the EU AI Act, the GDPR (and corresponding national data protection frameworks), existing equality and employment laws, and codetermination/consultation rules - with many stakeholders urging time for implementation and simplification rather than more rules.

It would be interesting to understand what this 'mix' of regulation looks like. Given the significant developments in the EU, perhaps we should start there.

The EU's prescriptive, rules-based model is now crystallised via the AI Act's risk framework, with most employment-related use cases tending toward "high-risk," and meaningful deployer obligations on employers (e.g. proper use, monitoring, worker information, AI literacy) set to bite in phases through 2026 and beyond.

Nevertheless, national labour frameworks continue to do real work illustrating that existing, technology-agnostic employment and equality laws still regulate outcomes irrespective of whether AI is used.

In our report, do you get a sense of whether this regulation across the EU does an adequate job of protecting employees when it comes to the use of workplace AI?

There appears to be a general perception amongst the surveyed EU practitioners of at least a “meaningful” baseline of protection, with many regulatory gaps tied to implementation detail (transparency, auditability, contestability) that the AI Act is expected to address as it fully applies. In this respect, my feeling is that the core challenge for countries across the EU is execution and enforcement, not legal absence.

With the EU AI Act set to continue its phased implementation, in what areas do you expect to see key EU policy debates on AI regulation in 2026?

Rather than layering new regimes, the near-term policy debate in Europe appears to be centring on streamlining as evidenced by the Commission’s “Digital Omnibus” proposals. These would adjust the AI Act’s timelines, expand sandboxes, reduce paperwork for non-high-risk tasks, and clarify GDPR rules on automated decision-making and AI model training - all to make compliance clearer and more innovation-friendly. Some suggest that this is symptomatic of a ‘Washington effect’, namely that the EU feels the need to react to a possibly more flexible and ‘pro-AI’ approach sought at a federal level by the current US administration.

As these proposals move through the EU’s legislative process, it will be interesting to see how the discussions play out alongside a fast-moving regulatory picture on AI outside of the EU, what changes (if any) will be mooted to the proposals, and where the EU will ultimately land when it comes to simplifying its digital rulebook.

And how about outside the EU, what trends have you observed there when it comes to the regulation of AI in the workplace?

Outside the EU, and from the data in our report, it appears that major EME jurisdictions skew towards being more

principles-led: the UK, Israel and Turkey all lean on existing data protection, equality and employment law frameworks, and extensive regulatory guidance, rather than a sweeping AI statute, yet converge conceptually on transparency, accountability, and human oversight. That said, Switzerland and Kazakhstan are moving toward general AI laws, underscoring that non-EU EME is not regulation-free but is sequencing legislation behind principles and existing frameworks.

For multinational employers in the region, this web of various protections and regulations could seem difficult to navigate. In your experience how are employers tackling this landscape?

The "Brussels effect" still matters: global employers are already coalescing around EU-style guardrails as an internal gold standard, even in non-EU markets. At the same time, the potential "Washington effect" that I mentioned earlier highlights geopolitical pressure to simplify and avoid overburdening innovation.

In practice, many multinational employers will adopt a single, jurisdiction-agnostic governance baseline - often an "EU AI Act-lite" approach blended with UK-style principles - to avoid a fragmented patchwork of policies across countries.

What should be the priority for policymakers moving forward in this space?

There is already "more than enough" protection in EME if existing law and guidance are implemented well. The priority should be consolidation, clarity, and proportional enforcement, not constant accretion of new governance obligations.

Finally, do you have any practical pointers for clients based in the region on using AI at work?

When thinking about practical steps for employers in the region, several stand out as being key. One is the need to **calibrate governance by risk and use case**. Some workplace tools are low-risk and operational (such as transcription or scheduling), so having a triage process that fast-tracks these while reserving full controls for "high-risk" employment uses in line with the EU AI Act is essential. Alongside this, accountability is critical. A named senior executive, ideally at Board level and with the relevant skills and experience, should be tasked with overseeing AI and its use within the organisation.

It is equally important for organisations to **map their AI estate**, because you cannot govern what you cannot see, and you cannot risk-assess, or where appropriate mitigate, what you don't know you have. Many multinational employers are also considering whether to adopt a **global or local operating model**; in practice, a single high-bar baseline (for example, EU-Act-aligned and UK-principles-informed) tends to reduce friction and satisfies expectations across markets that are converging on similar concepts of transparency, human oversight, and non-discrimination.

Employers should continue to **anchor to data-protection fundamentals**, ensuring lawful bases, transparency, purpose limitation, accuracy and rights management for any AI-enabled processing, mindful that GDPR and UK data-protection regimes already impose safeguards for significant automated decisions. They should also work to **embed explainability and worker information as defaults and strengthen algorithmic accountability** by providing clear notices of AI use, meaningful explanations where decisions affect individuals, and practical routes to contestability and human review. Documentation, logging, testing and monitoring are crucial to support bias mitigation and audits, anticipating the AI

Act’s technical record-keeping ethos and helping close the gaps identified by EU practitioners.

Another key element is investment in **AI literacy and change management**, ensuring HR, legal, compliance and frontline users are trained on safe operation, bias risks and escalation paths - an explicit expectation for providers and deployers under the EU AI Act and a practical control everywhere. At the same time, organisations should **engage social partners strategically**; where works councils or collective bodies exist, brief and consult early on AI deployments. Jurisdictions like Germany illustrate how co-determination and information rights intersect with AI rollouts.

There is also significant value in **tightening vendor management**, ensuring contracts include transparency obligations, data provenance, performance metrics, bias-testing support and audit cooperation, reflecting the provider/deployer split in the AI Act and the practical need to evidence controls across the supply chain.

Finally, organisations need to **plan for timelines and flexibility - and be prepared**. This includes tracking the phased application of the AI Act and emerging “Digital Omnibus” simplifications, making use of regulatory sandboxes and real-world testing where available, and periodically refreshing controls as standards and guidance mature. Crucially, an AI incident-response strategy should be in place to deal with not only outages and breaches but also model misbehaviour, harmful outputs, fairness failures, data leaks, data poisoning and systemic drift that can materially degrade performance.

RENATA BUERÓN

Associate at Ius Laboris Mexico specialising in Privacy and Data Protection and Information Technology

How would you describe the regulatory landscape in the Americas region when it comes to the use of AI in the workplace?

Across the Americas, there is no single, unified "AI in employment" law, nor is the region converging toward a single, harmonised regime as we are seeing in the EU with the EU AI Act. Rather in practice, the use of AI and data-driven tools in the workplace is governed through a combination of national privacy, labour, anti-discrimination, and consumer protection frameworks, which together define what companies can and cannot do when deploying technology that affects workers.

If I were to go slightly more granular, regulation broadly tends to be privacy-led rather than AI-led across the region (certain in Latin America), with automated decision-making assessed primarily through data protection and fundamental rights frameworks.

There are then also specific jurisdictional nuances that emerge, such as the distinctive state-by-state regulatory approach in the United States.

And what would you say is the knock-on effect of this approach to employers in the region?

It means that companies operating across the Americas should view workplace AI not as a purely technical or HR issue, but as a governance issue that sits at the intersection of privacy, labour, compliance, and organisational culture.

As a result, decisions about deploying AI in the workplace - particularly in Mexico - should not be taken solely by IT or HR functions, but should involve privacy, labour, and compliance teams together, to ensure that technology supports productivity without undermining employee trust, well-being, or legal compliance.

An example of this is the way that workplace monitoring and algorithmic oversight are increasingly viewed not only as privacy issues, but also as issues of employee well-being and organisational health. Mexico is particularly notable in this respect because NOM-035 (Mexico's official workplace psychosocial risk prevention standard) requires employers to identify, prevent, and mitigate psychosocial risk factors and to promote a favorable organisational environment. These obligations become especially relevant when companies use AI for continuous monitoring, productivity scoring, or behavioral analytics that may increase stress, pressure, or a sense of constant surveillance.

You referred previously to the EU AI Act. To what extent has this framework influenced the approach to regulation in the Americas region?

Globally, the EU AI Act has become the reference architecture for AI governance, particularly through its risk-based approach, documentation requirements, and emphasis on human oversight. Regionally, in the Americas, and while the Act is not directly applicable, its structure increasingly influences regulatory thinking, corporate governance models, and expectations of responsible use of AI.

I think this is apparent from the findings in the report whereby several jurisdictions in the region, including Mexico, appear to be in an early transition stage from relying solely on existing legislation that incidentally applies to AI systems, towards developing initiatives that would establish a more structured regulatory framework. This shift is reflected in the various legislative proposals highlighted, as well as existing, AI-specific legislation already in force in countries such as Peru. Many of these introduce risk-based approaches to AI regulation, inspired by the EU AI Act.

Even so, this influence is being adopted selectively rather than wholesale. Certain jurisdictions and policy initiatives reflect elements of the EU model - such as treating employment-related AI as high-risk, requiring transparency or audits, or emphasising accountability - but as I mention above, the region is not converging toward a single, harmonised regime.

You've already shared some practical pointers for employers using AI in the workplace. Are there any additional tips you'd highlight for employers in the region?

From the very start, employers should **map where and how they use AI** in the workplace - across recruitment and screening, performance and productivity management, monitoring, scheduling, terminations, IT-security tools and any employee-facing systems. For each use, it is helpful to note how automated it is, how much it affects people, what type of data it relies on, and whether the tool comes from a vendor or is built internally. This simple exercise gives employers visibility and control in what is still a fragmented regulatory environment.

Another key, primary consideration is **transparency planning**. Employers should understand and prepare for transparency requirements early on. In many countries, employers will need to explain to candidates and employees that automated tools are used, what kind of data they rely on, and how people can request more information or alternative processes. Having this prepared in advance avoids last-minute fixes and builds trust. Closely linked to this is **risk analysis**. Any AI that influences employment decisions should be treated as high risk by default. Even where the law does not formally label it that way, regulators, courts and employees often will. Ensuring meaningful human review, clear criteria behind decisions, opportunities for people to ask questions or raise concerns, and regular checks for unfair or unintended outcomes is key.

Employers should also prioritise **vendor management**, working with vendors as partners in risk rather than simply as suppliers of technology. Contracts should provide real insight into how the system works, what its limits are, how data is used, how bias is tested and how incidents are handled. Caution is needed with arrangements that shift responsibility away from the vendor simply because a human formally clicks "approve."

Finally, **consistent record-keeping** is critical. Employers should test, monitor and document frequently and consistently, keeping a straightforward internal record for each tool explaining what it does, what data it uses, how it is evaluated and how it is overseen by humans. This is not only good governance, it also becomes extremely valuable if a decision is later questioned.

LIONEL TAN

Partner at Ius Laboris Singapore specialising in Technology, Media and Telecommunications, and Data and Digital Economy

Firstly, how would you sum up the overall picture on workplace AI regulation in the region?

The workplace regulations on AI in the Asia Pacific region are not uniform but some common threads may be observed. Most jurisdictions combine soft-law guidance with existing statutes, while a few have enacted or enforced targeted AI or algorithmic rules. Employment-facing AI is primarily constrained through data protection, anti-discrimination, surveillance and monitoring, along with sectoral requirements, with increasing emphasis on transparency, auditability, and testing.

Is it possible to draw any similarities with other regions?

In the APAC region, the countries generally aim at achieving similar outcomes as the EU, the UK and the US – namely, fairness, transparency, safety - but often via existing regulatory regimes and soft law rather than a single horizontal AI statute.

Nevertheless, even without explicit AI statutes, where AI is used for the workplace in a way which may have a significant impact, there will invariably be requirements of assessments, explainability, bias controls, 'human-in-the-loop' and robust vendor management. Compared with Europe and the US, data localisation, security assessments, and cross-border transfer requirements can be more determinative, especially in China and increasingly in other jurisdictions within the APAC region.

Finally, what key practical pointers would you suggest employers in the region adopt when it comes to the use of AI in the workplace?

Before the deployment of workplace AI, employers should **use representative datasets** to carry out checks to ensure fairness and robustness and to remove bias. Local and cultural contexts, including multilingual inputs, should be taken into account, and systems should be retested periodically to continue to verify performance. Auditable records should also be kept.

When deployed, employers should **create an inventory of AI-enabled processes**, such as CV screening, productivity scoring and chatbots, and classify the risks by their impact on individuals' rights and livelihood. Higher-risk activities, particularly hiring, performance evaluation, termination and monitoring, should receive particular attention. **Human oversight** should also be built into these AI-enabled processes so that a human decision-maker can review, override and document the rationale for decisions.

Organisations must also **ensure adherence to workplace privacy and/or surveillance rules** and regulations, which may differ across jurisdictions in the region, and must satisfy all consent and notice requirements. They should also be familiar with and **cross-border data and localisation issues** and ensure compliance with the same, planning for data localisation or on-premises/virtual-private deployment if necessary.

In addition, employers should **conduct research and evaluation of AI vendors**, ensuring that there are rights of audit and update commitments. Paying close attention to IP and confidentiality clauses, data-breach co-operation and rights to suspend or terminate agreements for non-compliance are also key.

Finally, an **AI governance committee** should be established, comprising representatives from Legal, HR, Privacy, Security and Risk Assessment. For potentially high-impact use cases, robust DPIAs should be conducted, with periodic reporting to senior stakeholders and management.

INTERNATIONAL POLICY GROUP

ARGENTINA
Ignacio Funes de Rioja

AUSTRALIA
Jessca Tinsley

CANADA
Sonia Regenbogen

GERMANY
Burkard Göpfert

ISRAEL
Liat Shaked-Katz

SPAIN
Román Gil Alburquerque

UNITED STATES
William J. Milani

UNITED KINGDOM
James Davies

CENTRAL TEAM

EXECUTIVE DIRECTOR
Sam Everatt

HEAD OF RESEARCH, CONTENT, AND LEARNING
Deborah Ishihara

SENIOR RESEARCHER
Susanna Gevorgyan

PROFESSIONAL SUPPORT LAWYER
Alex Scott

CONTRIBUTORS

AUSTRALIA
Alice DeBoos
Jessica Tinsley
Nihara Perera

BULGARIA
Deyan Terziev

CHILE
Marcela Salazar
Rodrigo Ibáñez

COLOMBIA
Catalina Santos
Andrés Fernández de Castro Muñoz

CROATIA
Andrej Žmikic
Jasna Belcic
Anella Bukovic

CZECH REPUBLIC
Michal Peškar
Jakub Lejsek
Natálie Mikolášková

DENMARK
Elsebeth Aaes-Jørgensen
Selma Carøe

FINLAND
Jukka Lång
Mika Kärkkäinen
Oskari Paasikivi
Eva-Lotta Hokkonen
Kristiina Paavilainen

GERMANY
Jessica Jacobi
Jakob Friedrich Krüger

GREECE
Dimitrios Kremalis
Zoi Tsagkou
Panagiota Gantzoudi

HONG KONG
Gladys Ching
Tanya Mirchandani

IRELAND
Linda Hynes
Megan Hurley

ISRAEL
Liat Shaked-Katz
Keren Assaf

ITALY
Paola Pucci
Mauro Gallo
Patrizia D'Ercole

KAZAKHSTAN
Yulia Chumachenko
Alexandr Chumachenko

LUXEMBOURG
Marie Behle
Elisabeth Collin

MALAYSIA
Selvamalar Alagaratnam
Foo Siew Lee

MEXICO
Renata Buerón Valenzuela

NETHERLANDS
Philip Nabben

NEW ZEALAND
Peter Kiely
Anthony Kamphorst

PERU
Luis Vinatea
María Pía Romero

POLAND
Michalina Kaczmarczyk

ROMANIA
Roxana Abrasu
Iurie Cojocaru
Bianca Arhire

SINGAPORE
Lionel Tan

SWEDEN
Petter Wenehult
Malin Berndal

SWITZERLAND
Thomas Pietruszak
Pascal Steingruber

TÜRKIYE
Batuhan Sahmay
Ipek Pekdiri
Merve Atayurt

UNITED KINGDOM
Alexander Milner-Smith
Sean Illing
Sam Berriman

UNITED STATES
Brian G. Cesaratto
Susan Gross Sholinsky

CONTACTS

ARGENTINA
Rodrigo Funes de Rioja
rodrigo.funes@bruchoufunes.com

AUSTRALIA
Alice DeBoos
alice.deboos@kingstonreid.com

AUSTRIA
Gerald Burgstaller
gerald.burgstaller@bpr.at

BAHRAIN
Samir Kantaria
s.kantaria@tamimi.com

BELGIUM
Chris Engels
chris.engels@claeysengels.be

BRAZIL
José Carlos Wahle
jose.wahle@veirano.com.br

BULGARIA
Borislav Boyanov
b.boyanov@boyanov.com

CANADA
Greg McGinnis
gmcginnis@mathewsdinsdale.com

CHILE
Enrique Munita
emunita@munitaabogados.cl

CHINA
Zheng Xie
zxie@fangdalaw.com

COLOMBIA
Catalina Santos
csantos@bu.com.co

CYPRUS
George Z. Georgiou
george@gzg.com.cy

CROATIA
Emir Bahtijarevic
Emir.Bahtijarevic@dtb.hr

CZECH REPUBLIC
Nataša Randlová
randlova@randls.com

DENMARK
Yvonne Frederiksen
yvonnefrederiksen@norrbomvinding.com

ESTONIA
Karina Paatsi
karina.paatsi@cobalt.legal

FINLAND
Seppo Havia
seppo.havia@dittmar.fi

FRANCE
Guillaume Bordier
gbordier@capstan.fr

GERMANY
Alexander Ulrich
alexander.ulrich@kliemt.de

GREECE
Konstantinos Kremalis
kkremalis@kremalis.gr

HONG KONG
Catherine Leung
catherine.leung@lewissilkin.com

HUNGARY
Hedi Bozsonyik
hedi.bozsonyik@bozsonyikpartners.com

INDIA
Rohit Kochhar
rohit@kochhar.com

IRELAND
Síobhra Rush
siobhra.rush@lewissilkin.com

ISRAEL
Liat Shaked-Katz
shaked@herzoglaw.co.il

ITALY
Valeria Morosini
valeria.morosini@toffolettodeluca.it

JAPAN
Kazutoshi Kakuyama
kazutoshi.kakuyama@amt-law.com

KAZAKHSTAN
Yulia Chumachenko
y.chumachenko@aequitas.kz

LATVIA
Toms Šulmanis
toms.sulmanis@cobalt.legal

LITHUANIA
Jovita Valatkaite
jovita.valatkaite@cobalt.legal

LUXEMBOURG
Guy Castegnaro
guy.castegnaro@castegnaro.lu

MALAYSIA
Selvamalar Alagaratnam
SA@Skrine.com

MALTA
Matthew Brincat
mbrincat@ganadoadvocates.com

MEXICO
Jorge De Presno
jorgedepresno@basham.com.mx

NETHERLANDS
Philip Nabben
p.nabben@bd-advocaten.nl

Corine Hoekstra
corine.hoekstra@bvza.nl

NEW ZEALAND
Peter Kiely
kiely@ktc.co.nz

NORWAY
Claude Lenth
cal@hjort.no

PERU
Luis Vinatea
lvinatea@vinateatoyama.com

POLAND
Katarzyna Dobkowska
katarzyna.dobkowska@raczkowski.eu

PORTUGAL
Inês Reis
ines.reis@pbbr.pt

ROMANIA
Roxana Abrasu
roxana.abrasu@nndkp.ro

SAUDI ARABIA
Mohsin Khan
mohsin.khan@tamimi.com

SERBIA
Milena Papac
milena.papac@karanovicpartners.com

SINGAPORE
Desmond Wee
desmond.wee@rajahtann.com

SLOVAKIA
Dusan Nitschneider
nitschneider@nitschneider.com

SLOVENIA
Darja Miklavcic
darja.miklavcic@selih.si

SOUTH KOREA
Chris Mandel
cmandel@yulchon.com

SPAIN
Román Gil
rga@sagardoy.com

SWEDEN
Jenny Hellberg
jenny.hellberg@elmzell.se

SWITZERLAND
Roberta Papa
roberta.papa@blesi-papa.ch

THAILAND
Piroon Saengpakdee
piroon.s@rajahtann.com

TURKEY
Batuhan Sahmay
batuhan.sahmay@bener.com

UKRAINE
Oksana Voynarovska
voynarovska@vkp.kiev.ua

UNITED ARAB EMIRATES
Samir Kantaria
s.kantaria@tamimi.com

UNITED KINGDOM
James Davies
james.davies@lewissilkin.com

Michaela Berry
michaela.berry@sackers.com

UNITED STATES
David W. Garland
DGarland@ebglaw.com

URUGUAY
Matías Pérez del Castillo
mperezdelcastillo@pdelc.com.uy

ENDNOTES

[1] European Parliament. (2023, June 8; updated 2025, February 19). EU AI Act: First regulation on artificial intelligence. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[2] International Association of Privacy Professionals (IAPP). (2025, July 29; updated 2026, January 14). EU AI Act regulatory directory. https://iapp.org/resources/article/eu-ai-act-regulatory-directory

[3] Draghi, M. (2024). The future of European competitiveness-A competitiveness strategy for Europe. European Commission. https://commission.europa.eu/topics/competitiveness/draghi-report_en

[4] Bologa, A. (2025, July 8). The Washington effect? Europe weighs pausing the AI Act. Center for European Policy Analysis. https://cepa.org/article/the-washington-effect-europe-weighs-pausing-the-ai-act/

[5] Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

[6] Chen, J. Brian. (2025, June 25). The "Washington effect" decides the AI race. The Japan Times. https://www.japantimes.co.jp/commentary/2025/06/25/world/washington-effect-decides-ai-race/

[7] Information Commissioner's Office. (2026, January 8). ICO tech futures: Agentic AI (Version 1.0.0). https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation//

[8] Information Commissioner's Office. (2025, June 25). Preventing harm, promoting trust: Our AI and biometrics strategy (Version 0.0.28). https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/artificial-intelligence-and-biometrics-strategy/

www.iuslaboris.com

info@iuslaboris.com

in /iuslaboris

Global HR Lawyers
Ius Laboris