HIRE RIGHT®

EMEA Compliance eBook

The Impact of AI on the Employment Process

The Impact of AI on the Employment Process

Table of Contents

Foreword

In recent years, we've seen more and more people taking their first steps into the world of AI. Whether this initial exploration is through work or in our personal lives, there is a common question many of us are trying to figure out: which AI tools or technologies should we be getting excited about and of which we should be wary?

At HireRight, we've been looking at the impact of AI on the employment process quite closely for some time because of the potentially big impact it could have on our business—as well as that of many, if not most, of our customers.

This eBook provides a high-level overview of some of the legislation, use cases, and key considerations associated with AI tools being used in the employment process—specifically within the EU and the UK.

First, we look at the EU Artificial Intelligence Act 2024 (EU AI Act), providing an overview of the act, its four risk-based categories of AI systems, and the enforcement and implementation timelines associated with it.

Next, we move on to the UK's approach to AI, how it compares to the EU's approach, and what any disparity between regulations may mean for companies with workers in both locations. Then, we cover how to prepare for the world of AI, with a focus on AI strategy and governance and a five-step guide of practical tasks to undertake.

Finally, we conclude this eBook by exploring some of the ways AI tools can be used in human capital management (HCM) and background screening, and some of their key benefits.

I hope that you find this eBook insightful and that it provides you with some food for thought regarding how AI tools could impact the role of HR within your business in the years to come.

Caroline Smith

VP, Deputy General Counsel
at HireRight

Chapter 1 - The EU AI Act

Introducing the EU AI Act

The EU Artificial Intelligence Act 2024 (EU AI Act) in some ways has similarities to the General Data Protection Regulation (GDPR)—it was quite a long time in the making and it was being talked about for at least a couple of years before it finally came into force.

In August 2024, the EU AI Act officially came into effect, but it will be applied incrementally over the next three years. The act itself is a rather chunky text at around 150 pages long—so you'd be forgiven if you've not yet spent the time going through it in detail. As with a lot of EU legislation, we find that we get this sort of overarching text to begin with but then what we're really wanting to see—and have clearly explained—is how we can apply this in the real world.

In the coming months, we expect to see the introduction of standards, codes of practice, and then also further guidance being issued. For that reason, a lot of what we cover in this eBook is going to be inevitably quite high level because, at the time of writing, we just don't know the details yet. (We will provide more updates on our blog when further information about the act is available.)

To begin with, we just have the framework. So, what are the regulatory obligations of the EU AI Act? Well, there are two types of operators: **AI system providers** and **deployers**.

It is important to know the difference between these two operator types and which one of these identities applies to your company in any given scenario because there are different regulatory obligations that will apply in each case.

- A **system provider** is the developer of an AI system or an entity that commissions its development and offers it to the market under their own name or trademark.
- A **deployer** is the user of an AI system (except in cases where the AI system is used for personal, non-professional activities).

Now, most HR professionals reading this will probably think your company is going to be a deployer because they are the users of an AI system. So, for example, if you are using a piece of AI technology you have bought from a third party you would typically be a deployer. But businesses could also sometimes fall into that provider definition if they develop their own AI systems or commission the development of any AI systems that are deployed under their own name or trademarks.

Extraterritorial Effect

By now, businesses are generally used to the GDPR and the extraterritorial effect that the GDPR has. This means that if you're processing any data of an EU resident, then the GDPR is going to apply regardless of where you, the entity, are located.

The EU AI Act also has extraterritorial effects, but these are a little bit different from the GDPR's. Like the GDPR, these extraterritorial effects apply to operators that are located both within and outside the EU. However, they also cover any AI system that's placed on the EU market or is put into service or used in the EU, or whose use may affect people in the EU—in that the input from the AI system is to be used in the EU. This means that if you're using an AI tool, for example, in your recruitment processes in the U.S., and you're going to recruit individuals from the EU, then the use of that AI system would not be subject to the EU AI Act, unlike the GDPR, which would be because the individuals currently reside within the EU.

This subtle difference from the GDPR may make it a bit more difficult for organisations to figure out what kind of AI they can use across the board in all their different locations because different rules are going to apply.

Defining Artificial Intelligence (AI)

According to the EU AI Act, an AI system is "a machine-based system that is designed to operate with varying levels of autonomy, and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the inputs it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

One of the areas we expect we're going to get more guidance on from the EU itself is what AI actually is—and this definition may change as we move through the three-year implementation.

A Risk-Based Approach to AI

So how does the EU view artificial intelligence? Well, it takes a risk-based approach, which at its simplest level classifies AI systems into four different categories: **1) prohibited, 2) high risk, 3) limited risk, and 4) general purpose AI models (GPAIs)**, each with a different regulatory approach.

A **prohibited AI system** includes any AI that is used for cognitive behavioural manipulation, emotion recognition in the workplace and educational institutions, and any type of social scoring. More information on prohibited AI systems can be found in Chapter 2 of the EU AI Act. These types of AI systems are going to be banned under the EU AI Act—so nobody operating within the EU is going to be able to use these types of AI from 2 February 2025.

Next, we have **high risk AI systems** and **limited risk AI systems**. These are the two categories that we are most likely to come across in our businesses and our everyday lives. We already know that the EU is going to consider most tools that we use in an HR environment to be "high risk" because they present a significant potential risk to health, safety, and fundamental rights. Effectively what they're saying is that any AI tool you use in recruitment determines whether somebody is going to get a job, or will be considered for a job, and therefore it affects their fundamental rights and is processing their personal data.

We expect that that most of the AI tools that HR professionals would use are going to be classified as high risk AI systems—and this is where we see the greatest amount of regulation. There are going to be requirements around:

- ✓ **datasets and data governance**
- ✓ **documentation and recordkeeping**
- ✓ **human oversight (at the end of any process)**
- ✓ **robustness, accuracy, and security; and**
- ✓ **a conformity assessment.**

A conformity assessment acts like a safety label in a similar fashion to what you would find on a household electrical appliance to show that it's been properly tested and is fit for purpose. If you're out in the market looking for any of these AI tools over the next couple of years, you should be pretty safe if you're buying one that has got one of these conformity assessments, because you know that it meets the requirements of the EU AI Act.

However, conformity assessments will not be required until August 2026—see the implementation timeline later in this chapter.

Limited risk systems would include chat bots and systems that create synthetic (computer-generated) content. There is not a lot of regulation for limited risk systems because it should be obvious that these systems are a kind of AI—for example, AI chat bots are often used by companies as a first line of customer service support to address common queries. So, providing you are being transparent around the use of AI, your obligations would be met.

The final category of AI systems is **general purpose AI models (GPAIs),** which would include things like ChatGPT and other generative AI tools. There are varying levels of regulation depending on whether the GPAI represents systemic risk or not. That systemic risk is defined in two ways: presumed or designated.

- **Presumed systemic risk** is where the model is trained using a computer power of more than 1025 FLOPS (floating point operations per second).
- **Designated systemic risk** is where the European Commission determines that the model presents systemic risk based on other criteria that indicate that that model has high impact capabilities. This may include things like the quality or the size of the datasets, the input and output modalities of that model (e.g. text to text for large language models), and its reach in terms of EU-registered business users and registered end users.

There are different regulatory obligations for GPAIs defined as having a systemic risk. If there is **systemic risk**, the GPAI is subject to greater regulatory obligations, including in relation to model evaluation and the assessment and mitigation of those systemic risks. If there is a **non-systemic risk**, there is a focus on transparency and then ensuring that the technical documentation requirements are met.

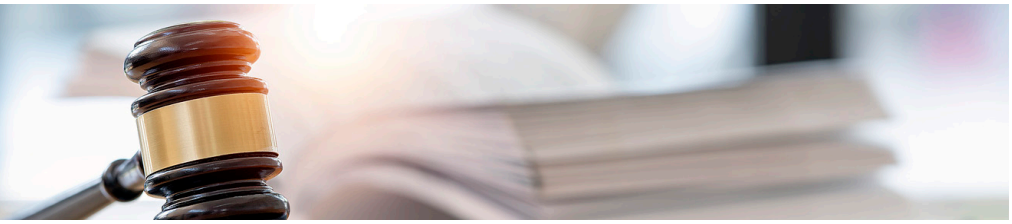
Additionally, all providers of GPAIs must also put in place a policy to comply with EU copyright laws—and you'll typically see that across these types of tools where it says something like "don't put anything in if you don't have the right to do so".

Enforcement and Implementation

The use of fines as a method of enforcement is quite common in the EU but what is interesting in this case is the different approach that's being taken by the EU. GPAIs are going to be enforced in a centralised manner via a newly formed "AI Office" creating a standardised way that the whole of the EU is going to look at these types of AI models.

However, for high risk AI or prohibited AI, this is going to be enforced by national supervisory authorities. So, what we might expect to see here is different regulators taking totally different views on what's prohibited or what's high risk or what will actually receive those conformity marks. This is a little bit contrary to where we have been trying to go with legislation like the GDPR, which has a more harmonious approach to implementation.

With this patchwork of laws that we're seeing with the EU, the UK, and the U.S., things like this make it even harder for organisations to really understand how they can comply and what decisions they need to make to comply. And, if you don't comply, those fines are quite high.



Fines

Infringements related to prohibited AI systems may reach **up to €35million** or **up to 7% of worldwide turnover** for the preceding financial year (whichever is higher).

Non-compliance with other obligations, including those related to the high risk AI and GPAIs, could incur fines of **up to €15million** or **up to 3% of worldwide turnover** for the preceding financial year (whichever is higher).

Interestingly, there are no lower limits as we see in the GDPR fines. This could be quite problematic when we're all trying to address our risk—for example if we are engaging with service providers. How do we measure that risk and account for these fines, which businesses are obviously going to want to try and ensure that they're not subject to from any regulator, especially with a lack of clarity in places between your deployer and your provider where there can be some crossover?

Implementation Timeline

The implementation timeline for the EU AI Act runs over a period of three years:

- **2 February 2025:** A ban on prohibited AI—so businesses will need to make sure they're not using any of those types of systems after that date.
- **2 August 2025:** GPAI obligations will come into force.
- **2 August 2026:** Most of those remaining obligations which include the specific, standalone, high risk categories and obligations, are going to come into force.
- **2 August 2027:** The obligations in relation to high risk AI systems that are products or safety components in products that are already subject to third-party conformity assessment requirements will come into force.

One thing that is potentially interesting about this three-year implementation period is that, with such a long timeline, what do we really think this legislation is going to look like in three years' time?

With technology advancing at an unprecedented pace, is what we consider to be high risk AI today still going to fall into that category in two years when this comes into force? It could have, in the time between now and then, become something universally accepted as normal. How is the EU going to respond to that and how are they going to change the legislation? This is an area that is sure to develop over the implementation period and I think it's likely that further guidelines will be issued to help employers navigate this ever-changing landscape.

Chapter 2 - AI in the UK

So far the UK has taken a rather different stance to the EU in respect to AI. The UK's previous government adopted a "wait and see" approach with a mandate for innovation because there was concern that legislating too early would stifle development and that the legislation could quickly become redundant.

However, the current Labour Government has a slightly different approach and in its manifesto stated that "binding regulation on a handful of companies developing the most powerful AI models" would be put in place. This was reiterated in The King's Speech (July 2024) as well post-election. Effectively the Labour Government has said that they will put regulation in place, but they're going to really home in on those organisations that are developing the most powerful AI models.

We think any forthcoming UK AI legislation is not going to be as all pervasive as the EU legislation, as it will be designed to support innovation—much like the UK Privacy Bill, which has also recently been put in front of Parliament. Additionally, the Government is currently looking to develop new sector verticals within the UK; one of these centres on digital identity and technologies surrounding that and another is around AI and really attracting entrepreneurs into the UK.

Looking ahead, we can expect to see some AI regulation introduced in the UK, but it is unlikely to be as stringent as the EU AI Act.

Regulating AI in the UK

So what AI regulations do we already have in place as we enter 2025? Well, the AI Safety Institute, a directorate of the UK Department for Science, Innovation and Technology, already exists. However, the Labour Government recently pledged to create a Regulatory Innovation Office (RIO). Again, on the same theme as before, the RIO should help the Government respond to fast-moving technology, supporting innovation and helping to approve new technologies faster.

This forward-thinking approach by the UK Government aims to take more of a middle ground position, striking a greater balance than the EU AI Act. However, for individuals based in the UK but whose work covers both the UK and the EU, it could be hard to determine what their organisation needs to do and which regulations they need to be aware of and with which they need to comply.

Beyond Europe, there are a lot of AI laws being debated in the U.S. and, up until recently, it looked like there was going to be some quite strong regulations introduced. However, we have seen that Donald Trump is more aligned to deregulating AI, so it will be interesting to see how things progress on this front during his presidency.

So, moving forward how are businesses going to navigate the various legislation effectively? Some may decide that as they must comply with the EU AI Act, they will also use that as the standard across the board. However, others might prefer a more nuanced approach so they can do more in certain locations, which may be dictated by the volumes of candidates you have and where you are actually hiring. It's certainly an interesting legal conundrum to try to figure out.

The Big Picture – AI Strategy and Governance

The first step to preparing for the world of AI is devising your company's AI strategy and you should begin by looking at the big picture. Organisations are going to utilise AI in different ways and some businesses lend themselves to using AI more than others. To get things started, businesses should be identifying their AI use cases and then the costs of implementation to help prioritise bringing those use cases into effect.

Once you have your strategy defined and documented, you can start to look at your governance framework. For example, at HireRight we've got an AI governance programme which includes myself and other members of our global compliance team, people who specialise in AI development, and, of course, our information security and IT teams.

It is important that businesses have that framework in place—and not just because it is needed for regulatory compliance.

Additionally, some of the areas that people are concerned with when they consider AI is whether it is fair or biased, what it does with their data, and how it may negatively impact people.

By having a governance framework in place, you can effectively show your employees—or anybody else, such as the talent that you are trying to attract—that you have a sensible, fair, legal use of AI, which can help you to build that trust within your organisation.

Next, training and/or a policy is required. This is critical because you can have lots of employees across your organisation that are looking at using tools to make their lives easier—or to work more efficiently—and they might not always recognise when AI is being used and what the implication of using that AI technology is.

It is important to train your team to understand what AI is, where they need to look out for it, and how they need to escalate it through your governance framework so that you have the right people looking at those tools and doing your AI assessments and your impact assessments. Some of you reading this might be used to your legal teams talking about data privacy impact assessments. We're going to have those being partnered with AI impact assessments, so it's really important that those things are identified and your teams really know what to look out for. Without proper AI impact assessments, there could be a risk of your employees using high risk or the prohibited AI, which could ultimately land your business in trouble if this is uncovered after the enforcement deadlines have passed.

Practical Tasks for Teams to Undertake

Many, if not most, businesses are by now already using AI tools in some capacity, either knowingly or perhaps inadvertently. For example, AI may be embedded in tools that are being used by your workforce, but the actual users could be unaware of the AI technology underpinning those tools. Here is a five-step list of practical tasks for your teams to undertake to help understand how AI is being used within your business.

1. **Perform an audit of current tools being used** plus any tools you may want to deploy soon to determine if they use AI.
2. If any of the tools being employed are using AI—and you are going to be using them within the EU—you need to **classify any AI tools against the EU AI Act risk categories:** prohibited, high risk, limited risk, or general purpose AI models (GPAIs).
3. Once you have classified any AI tools into these four categories, **perform a gap analysis to determine if each tool meets the requirements set out by the EU legislation** and, if not, identify what must be done to ensure those requirements are met. *(Note: We do not yet know all these requirements, and there may be some changes over the next three years. The legislation may currently contain gaps because until 2026 is not actually in force, so there is time to work with your providers to figure out what they are doing and how they intend to prepare.)*

4. **Review your existing suppliers and/or customers.** You need to determine if changes are needed in any contracts to ensure that the relevant requirements are being met and warranted against by your suppliers or you are giving warranties to your customers if you're deploying any AI tools in the services that you're offering them. If we look at the legislation at the moment, it's very difficult to know today exactly what it is that you put in a contract, especially around liability, because it is so broad, and we don't yet have all the guidelines.

   The other thing you don't want to do at this stage is to stifle your suppliers' internal development because the more stringent provisions you put in, the less likely it is that they're going to be able to develop AI tools or products utilising AI that ultimately will have some benefit to your business.

   It may be wise to keep requirements quite broad at this point or maybe even wait until we know which direction the legislation is heading in before taking any action.

5. **Continue to monitor developments in this area.** The EU AI Act is just one piece of legislation but there are lots more out there. Decisions may need to be made around which standards your company is going to apply across the board, and this may not be an easy decision for you to make. There could be some amazing tools out there that you could perfectly happily use in the UK or the U.S. but you might have a few more issues using them within the EU. Each business must determine what will work best for them and their needs, which may vary depending on where they operate and whether their candidates or employees are located within the EU.

Chapter 4 - Use of AI in HCM and Background Screening

The use of AI in any organisation must be fair and unbiased—so that's the first thing you need to consider. Once that has been established, there are many different applications of AI tools that could help businesses in a variety of areas, with many designed to drive efficiency—for example you could use an AI tool to:

- ✓ write better job descriptions for your company's vacancies—in a fraction of the time that a human would take
- ✓ look at all the CVs received for a job and use the keywords from the job description to match those things up to help quickly identify the best-suited talent to interview; or
- ✓ help identify hiring risks or retention risks within your organisation.

There is so much data available that could be analysed and there are various AI tools that can use this data and extract the value from it in ways that we just simply cannot do as humans, as there is simply too much data to process.

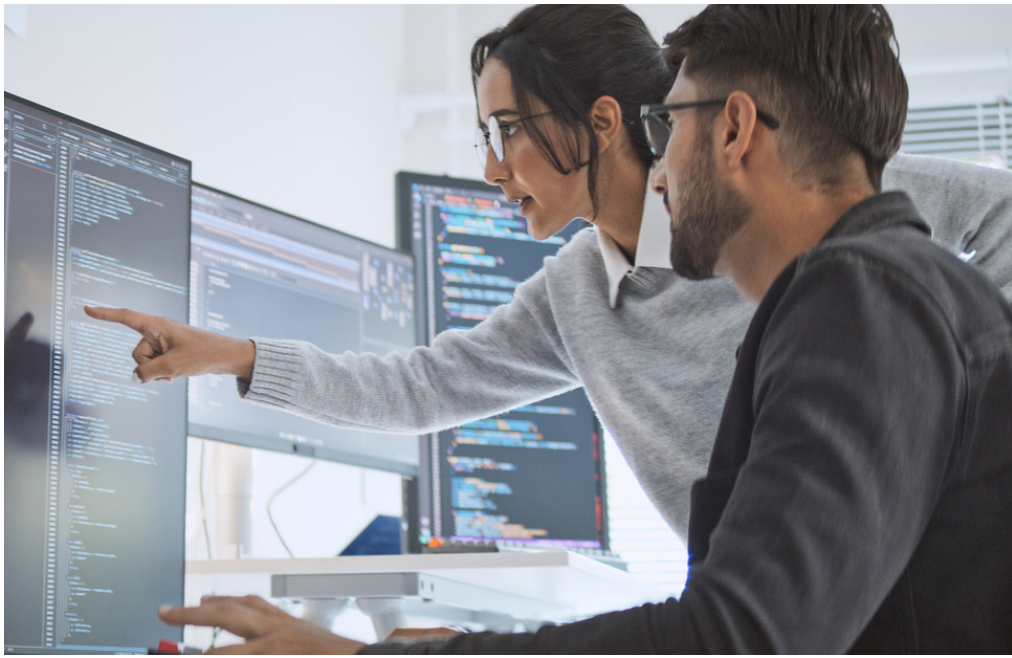
Interestingly, the Chinese Government has recently changed its laws so that companies can now include the data they hold as an asset on their balance sheets. This is indicative of what we are seeing more broadly, with more businesses acknowledging that their data is a valuable asset and, subsequently, viewing it in a different way.

Working with Large Data Sets

At HireRight, we're looking at how we can deal with large data sets. We don't currently have many products that utilise AI but one of our products that does is our Social Media Search. For this product, our customers provide us with keywords, which we pass on to our vendor, and then their AI tools use these to identify anything from the candidate or employee's public social media profiles and report back with a risk factor. Crucially, this process allows human intervention, which is critical from an EU perspective, because you can then have conversations with the individuals about anything found that causes concern to your business. Essentially, you are not making an employment decision solely based on that data.

The use of AI in this product means you are not having to manually search an individual's Facebook, X, and various other public online profiles for information when you are trying to screen somebody and onboard them as efficiently as possible. So, AI can really help when we are dealing with these types of large datasets. The same applies with HireRight's Adverse Media Search, which is a search of over 20,000 English-language online and printed media sources.

Anything with a large data set means that if there is just a pair of human eyes reviewing something, you are inevitably going to get more human error. In contrast, AI can help get through all that data much more quickly—and more accurately.



Chapter 4 - Use of AI in HCM and Background Screening

Using Automation

A common application of automation is for repetitive tasks. One of the things that HireRight is currently looking at is how we use robotic process automation (RPA) within our operations team to help allocate the work, for example adjudicating results, and using a chatbot to provide quick responses to frequently asked candidate questions, such as how to reset your password. This not only saves time, positively impacting their candidate experience, it also allows us to upskill our customer services team to deal with the more complex questions that candidates may have.

Driving Accuracy

AI can also be really useful for background screening companies like HireRight to help drive accuracy. One such example of this is name matching, which is really complex in certain jurisdictions that have Latin names such as the Philippines, anywhere in South America, Spain, Portugal, etc. In these locations, a woman will have her full name but if she gets married, she will move one name to the left, which can be difficult when it comes to name matching. But if you are using AI and algorithms then you can drive that accuracy and extract more value from the data because you can more accurately match the candidates.

New Opportunities

There is a lot of talk about replacing employees with AI. But one of the other things that HR professionals need to look at is their company's strategy around which AI tools they plan to deploy. They should also be considering the individuals that they already have within their business because there will likely be people with long tenures who really understand the business but might not have those skills right now. For these people, companies will need to identify who they want to keep. While their repetitive task jobs might be replaced, there may be a way to upskill those individuals to take on new roles or to use these new AI tools rather than simply replacing them.

Another opportunity that AI gives us is a whole raft of new jobs that even three or four years ago we just wouldn't have thought existed. As we discussed earlier, with new AI tools comes new requirements for governance, human oversight, and quality control into how they are used—functions that organisations didn't need before. So, as part of your company's AI strategy, you should be looking at what roles or jobs will be needed to support the use of any new AI tools, which may be an opportunity to retrain or upskill current employees rather than needing to hire in new people who may not know your business in the same way.

Candidates Using AI

One final consideration around the use of AI is your company's position on candidates using AI tools to support their job applications.

On the one hand, you may feel like any use of AI tools to potentially enhance a CV or covering letter is "cheating" and is potentially misrepresenting the candidate if it is not entirely produced by themselves. AI tools certainly could be used to create the "perfect" CV or covering letter for a job, which may not be an entirely truthful representation of the skills and experience the candidate possesses. Also, not all candidates will be familiar with—or comfortable using—AI tools, so does this mean that individuals using these tools have an unfair advantage?

But, on the other hand, long before AI, individuals have been tailoring details on their CVs to give them an advantage in the recruitment process. Is it fair to assume that anybody using AI tools to support their job applications is doing so to secure a job for which they are ultimately underqualified? You could also argue that a candidate's familiarity with AI tools is part of their skillset so why shouldn't they be allowed to use these tools to help put their best foot forward with their application?

Another viewpoint is that many employers are already using AI tools in the recruitment process—for example to help sift through high volumes of job applications to help identify the candidates that most closely match the job description— so why shouldn't candidates be able to use the tools they have available to them to ensure they stand the best chance of making it through to the initial selection process? If your company takes this stance, it is especially important that you have a robust interviewing process and pre-employment screening programme in place to help determine a candidate's suitability for a role and uncover any misrepresentation (e.g., if false claims were made about past employment, academic history, or professional qualifications).

Ultimately, it will be down to each organisation to determine if they are comfortable with their candidates using AI tools in their job applications or not and if not, how they plan to deter candidates from using them or detecting when they have been used. There is no right or wrong approach to this but, depending on how important it is for you to know if your candidates have used AI tools, you could address this topic with them within your job descriptions or during the interview process—or even consider tools to detect if AI has been used on your candidates' job applications.

Conclusion

AI is likely to have a huge impact on the employment process in the coming years—for businesses and candidates—so it is important to keep up to speed with the latest developments from both a regulatory and technological perspective.

I hope you found this eBook an informative introduction to some of the topics surrounding the use of AI tools in recruitment—including the EU AI Act, the UK's approach to AI regulation, preparing for the world of AI, and the uses of AI in human capital management and background screening—and that it gave you some actionable takeaways and topics for discussion among your teams as you plan your company's AI governance strategy for 2025 and beyond.

About HireRight

HireRight is a leading global provider of technology-driven workforce risk management and compliance solutions. We provide comprehensive background screening, verification, identification, monitoring, and drug and health screening services for approximately 34,000 customers around the globe. We offer our services via a global platform that tightly integrates into our customers' human capital management systems, enabling highly effective and efficient workflows for workforce hiring, onboarding, and monitoring. In 2024, we screened more than 60 million job applicants, employees, and contractors for our customers and processed more than 120 million screens.

For more information, visit www.HireRight.com.

Published March 2025

U.V.0325

CONTACT US

To get in touch, please go to
www.hireright.com/contact-us

FOLLOW US

linkedin.com/company/hireright

facebook.com/hireright