



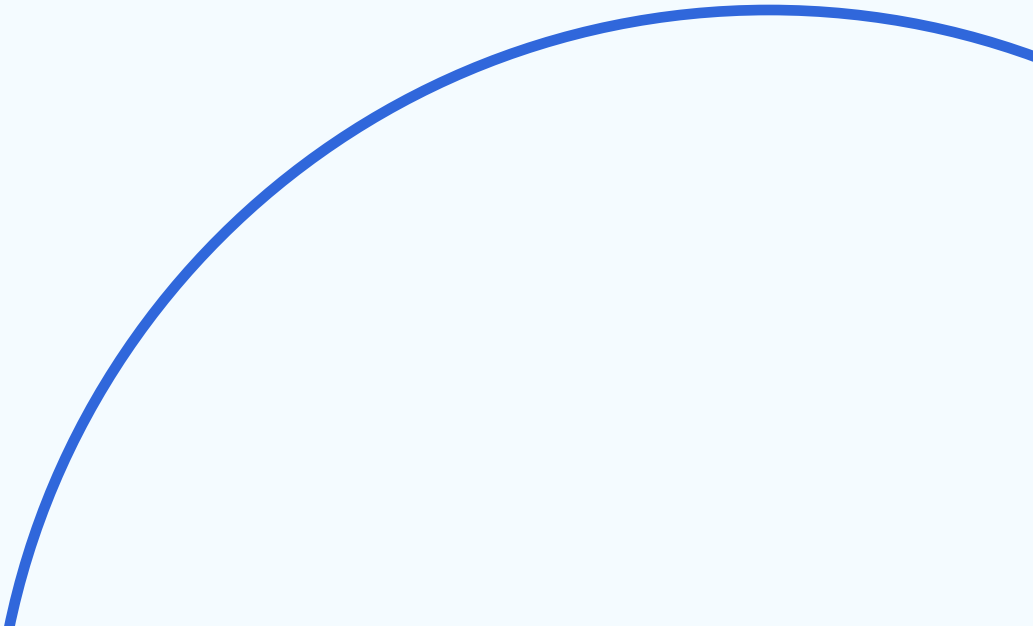
dayforce

GUIDE

The 5 non-negotiables of adopting AI for HCM

Contents

The 5 non-negotiables of adopting AI for HCM	3
Non-negotiable #1: Prepare your people	4
Non-negotiable #2: Get real about compliance	5
Non-negotiable #3: Use AI only where and when you require it	7
Non-negotiable #4: Break open the black box... where possible	8
Non-negotiable #5: Protect people and data	9
Moving forward	10
Sources	11



The 5 non-negotiables of adopting AI for HCM

If you're reading this, you're probably considering new investments in artificial intelligence (AI) to help improve your organisation's HCM efforts. You may already have a sense of what AI can help your workforce do, including:

- Generative AI assistants that can answer questions, find and summarise info, recommend actions or create original content from scratch.
- AI agents that can anticipate user intent, perform complex workflows, and simplify tasks¹
- ML-powered insights that can help predict business outcomes based on relevant, historical data

You may have even prioritised the use cases you want to move forward with and secured buy-in from key stakeholders. Now comes the hard part: choosing and implementing technology that can help you unlock the value of AI while helping you manage potential risks.

It's an exciting moment, but it's also where many organisations get stuck.

Too often, companies treat AI as a standalone capability they can layer on top of existing systems. But AI in HCM can't be assessed in isolation. Its effectiveness depends on the platform, data model, workflows, and governance structure underneath it. Without that foundation, even advanced AI can struggle to deliver reliable, scalable outcomes.

And when that foundation is fragmented or unclear, the risks can multiply. Data becomes harder to govern. Decisions become more difficult to explain. Compliance gaps become easier to miss. Security and privacy controls become harder to enforce consistently.

If these concerns sound familiar, you're not alone. According to SHRM's State of AI in HR 2026 report, privacy and security risks are the biggest technical barrier to expanding AI in HR.² When those concerns go unresolved, organisations can stall out on adoption or push ahead without the right protections in place. Either way, the result can be added legal, operational, and reputational risk for both employers and their AI providers.

Before you go looking for the right AI solutions, you need to understand the non-negotiables of adopting AI for HCM. This guide provides a helpful breakdown of each, so your organisation is better equipped to take its next step with more confidence.

Non-negotiable #1

Prepare your people

Mind the gap

Before you accelerate any AI initiative, you need to bring your people with you. AI will reshape not only day-to-day tasks, but also roles, responsibilities, and how work gets done. That means you need to build the literacy, confidence, and practical judgement people need to use AI effectively.

The skills gap is real. According to Skillsoft research, AI and machine learning remain a major skills gap for organisations, with many respondents pointing to employer support and training as part of the challenge.³ Many leaders appreciate this challenge, with 95% of surveyed IT leaders believing AI projects will fail without staff who can effectively use the tools.⁴ They have good reason to believe as much, as a Pluralsight survey found that 65% of surveyed organisations that had to abandon AI projects did so due to a lack of AI skills among staff.⁵

If you want AI adoption to succeed in HCM, that gap needs to be addressed early and often.

What to do about it

Effective, engaging training

Start by building tailored training programs for the people who'll interact with AI. Include practical guidance on responsible use, AI ethics, and when human judgement should take the lead. It's also important to communicate clearly that AI is there to support people in their work, not replace them.

Training should reflect how different roles will use the technology. A one-size-fits-all approach will only go so far. The more tailored and relevant the learning experience, the more likely people are to build confidence and use the tools well.

To scale that kind of targeted learning, it helps to use an enterprise learning management system that sits within your HCM platform rather than beside it.⁶ That makes it easier for learning leaders and managers to assign the right training, set timelines, track completion, and follow up where support is needed. It also makes it easier to use relevant workforce data across the employee lifecycle to measure adoption and improve the impact of training over time.

Build a sandbox

Once training is in place, give people a safe environment to practice. An AI sandbox is a controlled test environment where employees can use AI tools in ways that mirror real work without creating unnecessary risk.

That matters because confidence doesn't come from theory alone. It comes from trying, learning, adjusting, and seeing what works. A sandbox gives people room to experiment safely, build practical skills, and think more creatively about how AI can improve the speed and quality of their work. When it's time to roll out AI more broadly, your people will be better prepared to use it effectively and responsibly.



Non-negotiable #2

Get real about compliance

The ground beneath your feet is moving

AI is evolving quickly, often faster than the rules that govern it. What's acceptable today may be restricted tomorrow. That means your AI approach for HCM needs to help you manage compliance, not just now, but as requirements continue to change.

That challenge is already affecting uptake. In an NTT DATA report, around four in five respondents say uncertainty about government regulation gets in the way of AI investment and implementation.⁷ In a more recent NTT report, respondents cite security, governance, risk and compliance concerns around autonomous agents as the top short- to mid-term challenge to adopting AI in cloud-based solutions.⁸

The legal complexity grows even further if your organisation operates across multiple jurisdictions. Different regions may define risk, accountability, transparency, consent, and data rights in different ways. That makes it harder to move quickly without increasing potential exposure.

One practical way to respond is to prioritise vendors that can demonstrate experience supporting leading AI regulations, standards, and frameworks, including the EU AI Act, the General Data Protection Regulation (GDPR)⁹, Australia's Privacy Act 1988, New Zealand's Privacy Act 2020, ISO/IEC 42001, and the NIST AI Risk Management Framework (AI RMF). This can help you better position your AI initiatives to support compliance with widely recognised regulatory and industry frameworks. But it's also important to remember that other regional frameworks are constantly in development, meaning that your company's AI solution will need to offer flexibility to respond to evolving requirements to help you address applicable legal and regulatory obligations.

This is where you'll need to ask:

- **How are compliance considerations built directly into the AI solution?**
- **How does the solution help support your team in adapting to evolving compliance frameworks?**
- **Does it have a verifiable track record of helping organisations navigate compliance requirements?**

If you're asking these questions of a potential solution partner, request concrete examples. You need more than reassurance. You need evidence that the technology and operating model can help you meet evolving requirements.



Non-negotiable #2

Get real about compliance (continued)

You're walking through a minefield of potential bias

Bias remains one of the most persistent and sensitive concerns around AI in HCM. Employers, employees, regulators, and candidates all want to know whether AI-enhanced recommendations that inform human decision-making are fair, accurate, and defensible.

Take candidate screening as one example. If an AI-enabled tool filters out applicants based on patterns that create biased outcomes, your organisation may still bear responsibility for the impact. That's why it is critical to understand how a solution assesses fairness, how models are monitored, and how biased outcomes are identified and addressed over time.

When you ask providers about bias, many will tell you they take it seriously. But that's not enough. Ask how fairness is assessed. Ask how models are tested and updated. Ask what data is used, what controls are in place, and how issues are escalated if biased outcomes are detected.

These concerns extend far beyond recruiting. Bias can influence decisions across the employee lifecycle, from development opportunities and internal mobility to scheduling, performance, and workforce planning. And like many AI-related issues, standards and expectations continue to evolve. You need a solution that can help you manage change and support evolving requirements.

Your obligations won't end with compliance support

Managing legal requirements is essential. But responsible AI in HCM requires more than compliance support alone. Organisations also have an ethical responsibility to make sure their use of AI doesn't create harm for individuals, groups, or society more broadly.

That's why it matters whether your solution partner has a clear ethical framework that goes beyond the minimum requirements of any single market. At a minimum, that framework should reflect a commitment to:

- **Trust** – This includes a commitment to following the highest standards of privacy, security, transparency, reliability, and sustainability.
- **Employee focus** – This includes determining whether your use of AI empowers and assists people, helps reduce bias and builds accountability into every stage of the solution's lifecycle.

When you ask a provider about ethics, expect more than a set of written principles. Ask how those commitments are operationalised. Ask how they're embedded into product design, governance, testing, and deployment decisions. Responsible AI should show up in the technology itself, not just in the messaging around it.

Non-negotiable #3

Use AI only where and when you require it

AI can create real value when it's applied in the right place, under the right conditions, with the right controls. But that only works if you can be precise about where, when, and how it is used.

That may sound like a small detail, but it's not.

Some AI-enabled HCM systems only let organisations turn AI on or off at a broad system level. That can create serious problems if your business operates across regions with different legal requirements or across functions with different risk profiles.

What happens if AI use is permitted in one jurisdiction but restricted in another? Can you control usage at the regional level? If rules change in a specific market, can you adjust quickly without affecting the rest of the business?

In some systems, the answer may be no.

You should also think carefully about access and control at the user level. Do you want AI tools available to everyone, or only to certain users, roles, or teams? Can individuals toggle AI features on or off themselves? Can your organisation restrict use by workflow, geography, or use case? And can those choices be governed centrally while helping minimise operational friction?

If your AI solution doesn't support alignment with your business strategy, governance model, and regulatory obligations, the cost can be significant. You may end up walking back adoption, replacing tools, or slowing progress across the business. A more flexible, responsibly designed approach can help you adapt with more confidence as requirements and priorities change.



Non-negotiable #4

Break open the black box... where possible

Will your AI show its work?

AI can give your users useful nudges and recommendations that help take your company's decision-making to the next level. But how does the AI arrive at its conclusions? Is it like making a move on a chessboard that no human player can understand? Or can it offer a transparent accounting of how it arrived where it did?

The stakes of AI in HCM, of course, are much higher than a game of chess. Concerns of bias, privacy, security and ethics are everywhere. According to a Gartner study, fragmented technologies (25%) and lack of transparency for third-party AI solutions (20%) are major challenges to implementing AI in an organisation.¹⁰ So if you're planning to use AI in ways that will influence consequential decisions, you need to ask:

- **Can you and your solution partner explain how the model makes those inferences or influences decisions?**
- **Can you explain it at a general level? What about the level of one specific decision?**
- **Does the proposed solution inform users when AI is being used in the activity they're performing?**

- **If you're deploying AI in a customer-facing system, do you get consent? Is the consent recorded and auditable?**

These risks can vary by jurisdiction. Different regions may have different expectations around explainability, transparency and disclosure. In practice, that means some AI systems will be easier to govern and defend than others. Explaining how large language models generate and support outputs can be difficult, but it's still important to understand what level of transparency a provider can offer and where its limitations begin.

How do you help ensure quality over time?

The quality of AI's inferences and decisions it may inform extends beyond the issue of bias. Accuracy and reliability are essential for AI use cases, but not all AI solutions can maintain consistent performance over time. Does your proposed solution have any performance limitations that might affect its transparency? For example, can you provide stakeholders with visibility into the quality of your AI and the data it is working with?

On the topic of quality, you'll want to ask your solution partner whether they constantly check their AI models for "drift"? Drift is when your AI model's performance degrades over time as it encounters real-world data that's different from the data it was trained on. Your solution partner should be able to clearly explain how they monitor and update their models on an ongoing basis to help build trust in your AI quality and help you identify and address risks associated with performance degradation.



Non-negotiable #5

Protect people and data

The basics

If you've come this far, you've probably put some thought into how your proposed AI solution will help you support security and privacy for you, your company, your people, and your customers. This is where it's essential for your AI solution to follow Privacy and Security by Design methodologies for embedding privacy and security directly into information technology.¹¹ These methodologies help responsible AI solution providers design technology that can help identify and address privacy and security risks.

The stakes for protecting sensitive and confidential data in the context of AI in HCM couldn't be higher. And this responsibility does not sit with your organisation alone. IBM research found that 82% of surveyed executives view AI security as a shared responsibility across suppliers, providers, and partners.¹² At the same time, the biggest barriers they cite are complexity across multiple AI providers, the rapid evolution

of AI technologies, and limited visibility into AI provider security controls. That makes it critical to choose a solution partner that can clearly explain its security practices, governance model, and use of third-party providers — and back those claims with evidence.

To help address these concerns, here's a quick rundown of the core questions you should ask a solution partner:

- **Does your AI solution send data to third parties? Can you control or limit when that occurs?**
- **Does it train on private company data (either its customers' or anyone else's?)**
- **Does it train on public data?**
- **Are the models generally trained, trained only on your company's data or on all customers?**
- **Where are the models hosted?**

These considerations can be amplified in fragmented HCM environments, where data is spread across systems. A single-platform architecture and single data model can help simplify governance and support risk management.

Once you've got your answers, it's time to ask the vendor if they can back up what they say with hard evidence.

Where's the proof?

Some of the concerns covered above won't be new. But remember — when solution partners say they do X, Y and Z to help safeguard privacy and security, ask for proof. If your prospective partner tells you they definitely had the right to train and test their model on the data they used for training and testing, can they prove it? How about some documentation? Does the solution partner retain any of the data that'll be used by your AI model? How do they handle the privacy of that?

Proof, please. Can you request that they not use specific data for training purposes? What are you allowed to carve out and how can they confirm that they've honoured your request?

You'll also want to learn as much as you can about your solution provider's audit process for its AI governance and operations. Can they provide documentation? Have they got a formal third-party audit process? Would they be willing to submit to one? Have they performed a risk assessment on their models? If not, would they be willing to? These are all critical questions to help you assess and proactively address some of the biggest risks AI might pose to your organisation.

Moving forward

Organisations that pursue AI without laying the right foundation may still move quickly, but speed alone isn't the same as progress. To adopt AI responsibly in HCM, you need an approach grounded in governance, flexibility, transparency, security, and workforce readiness.

At a minimum, you need a solution partner that can help you support your approach to addressing the five non-negotiables of adopting AI for HCM. If a prospective partner struggles to answer the questions in this guide — or can't show how its technology supports them — take that seriously. It may be a sign that you need to keep evaluating your options.

AI can help your organisation improve productivity, strengthen decision-making, and create more value across the workforce. But to pursue those benefits, you need more than impressive features. You need an approach designed to support responsible, scalable adoption from the start.

Disclaimer: The information provided in this guide is provided for informational purposes only and should not be relied upon or construed as legal advice and does not create an attorney-client relationship. You should review with your legal advisors how the laws identified in this post may apply to your specific situation.



Sources

1. [Dayforce Announces Dayforce AI Agents, Dayforce, November 2024.](#)
2. [The State of AI in HR 2026, SHRM, 2026.](#)
3. [Sarah White, 74% of workers suggest employers to blame for their AI skills gap, CIO, October 2024.](#)
4. [Grant Gross, The real AI training gap? IT leaders believe in it, but many don't provide it, CIO, September 2024.](#)
5. [2025 Pluralsight AI Skills Report, Pluralsight, 2025.](#)
6. [How to close the skills gap with your enterprise learning management system, Dayforce, October 2024.](#)
7. [New NTT DATA Report Exposes the AI Responsibility Crisis: 81% of Business Leaders Call for Clearer AI Leadership to Avoid Risk and Support Innovation, NTT, February 2025.](#)
8. [Cloud-led innovation in the era of AI, NTT, 2026.](#)
9. [What is GDPR, the EU's new data protection law? Ben Welford. GDPR. EU, 2025.](#)
10. [AI governance frameworks for responsible AI, Gartner, 2023.](#)
11. [Privacy by Design, Information and Privacy Commissioner of Ontario, 2018.](#)
12. [Elusive threats, elastic defence: Securing AI at scale, IBM, 2026.](#)



Dayforce makes work life better. Everything we do as a global leader in HCM technology is focused on enabling thousands of customers and millions of employees around the world to do the work they're meant to do. With our single AI-powered people platform for HR, Pay, Time, Talent, Planning and Analytics, organisations of all sizes and industries are achieving simplicity at scale that creates compounding, quantifiable value for their people and business. To learn more, visit dayforce.com/au.

dayforce.com/au