



AI Due Diligence: 12 Questions to Ask Your HR Vendors

Buying AI-powered HR technology brings new considerations for procurement. Beyond understanding how HR teams plan to use AI in people processes and candidate workflows, organizations must also understand how those AI systems are built, tested, and governed under the [EU AI Act](#).

Some obligations are already in force, including rules on prohibited AI practices, AI literacy, and transparency. Others, including those specific to high-risk employment decisions, don't apply until December 2027. That timeline matters for due diligence: it shapes which questions are urgent now, and which your vendors should be preparing to answer.

Know your role

Under the EU AI Act, your vendor may be the AI provider, but your organization will still have responsibilities as the deployer. Vendor due diligence is therefore only one part of AI Act readiness so check out our [HR Checklist: Meeting Your Responsibilities as a Deployer of AI](#).

Together they give you a view of both sides of the Act; what your vendor is responsible for, and what you need to demonstrate.

These 12 questions are designed to help you cut through broad AI claims, know what to look for in a vendor's response and identify the evidence you should expect – helping you make more informed, confident AI purchasing and renewal decisions.

Understand the AI

This set of questions is designed to help you determine whether a product or solution falls within scope of the Act, and to clarify how AI is used within it.

What AI capabilities are included in your talent product?

This should help determine any use of AI by your vendor, even in background tasks or processing. Good vendors should have clear documentation of exactly where AI is used across the candidate or employee journey and be able to distinguish between AI-assisted features and fully automated decisions.

Is generative AI used?

Use this to confirm whether generative AI plays any role in the product, even in background tasks like drafting feedback or summaries. Good vendors should be able to specify where it's used and how outputs are checked for consistency across candidates.

Which models or providers are involved?

A strong answer will clarify whether the AI is built in-house, licensed from a third party, or a mix of both. Good vendors should be transparent about which models and providers are involved, as this affects who holds which compliance obligations.

Do you classify the talent product as “high-risk” under the EU AI Act?

This confirms whether the vendor has properly assessed their own product against the Act's risk categories, rather than assuming or asserting compliance. Good vendors should explain their classification and the reasoning behind it, not just state a conclusion.

Watch out for: Certification claims

There's no official 'EU AI Act compliant' badge vendors can display, but you can ask to see their conformity assessments and technical documentation, which show the work they've done toward compliance.

Understand the risk

Risk under the EU AI Act can show up in biased outcomes, decisions made without human oversight, and errors that go unmanaged. This set of questions is designed to help you understand how a vendor manages that risk.

How are bias and discrimination managed in your talent product?

Look for evidence of proactive bias testing, not just a policy statement. Good vendors should be able to share bias testing methodology, results across protected groups, and how often this testing is repeated.

What human oversight is required for decisions made or informed by your AI?

This confirms whether a human reviews and can challenge AI-informed outcomes. Good vendors should be able to describe what a reviewer sees and where they can override the AI's recommendation.

What governance is in place for changes to your AI model?

The goal here is to establish whether updates are tested and approved before release or rolled out without review. Good vendors should be able to provide AI governance documentation covering version control, testing, and how customers are notified of material changes.

If your AI gets it wrong, what happens next?

This surfaces whether the vendor has a defined incident management process or is relying on ad hoc fixes. Good vendors should be able to provide incident response documentation and evidence of any related risk assessments carried out.

If you hear: "Powered by advanced AI"

That's marketing language, not evidence. Ask what the AI does, where it's used, and how it's governed.

Understand the data

The EU AI Act requires you to understand how a vendor's product sources, uses, and retains your candidates' and employees' personal data. That's why we've put together this list of questions.

What candidate or employee personal data is processed in the talent product?

Look for a clear, specific list of data types processed, rather than a general assurance. Good vendors should be able to provide data processing documentation setting out exactly what personal data is collected and why.

Is customer data used to train AI models?

This confirms whether your candidates' or employees' data is being used to improve the vendor's models, which carries its own transparency and consent implications. Good vendors should be able to state clearly whether this happens, and under what safeguards.

Where is data stored?

This establishes where data resides and what security standards apply, which matters for both data protection and vendor accountability. Good vendors should be able to point to relevant security certifications and technical documentation supporting their storage practices.

What data retention policies apply?

The goal here is to confirm data isn't kept longer than necessary or disposed of in a way that undermines audit requirements. Good vendors should be able to share a documented retention policy that aligns with GDPR and their AI Act record-keeping obligations.



The image shows a document titled 'SHL Checklist: Meeting Your Responsibilities as a Deployer of AI'. It is a practical guide for navigating responsibilities under the EU AI Act. The document includes sections on 'What it means to be a Deployer', 'Practical steps to ensure compliance', and 'Two ways to ensure compliance'. It also features a 'SHL' logo and a 'Read the Vendor Questions' link.

Remember: choosing the right vendor is necessary, but it is not sufficient. The EU AI Act places obligations on deployers as well as providers. After completing this vendor assessment, refer to our **HR Deployer Checklist** for the practical actions your organization should take to support compliance.

Read the checklist for HR teams ➡➡