Brace for ai impact: from hype to risk – is your company ready?

KINSTELLAR

In 2022, we were writing about the promising but at the time still hypothetical impact of generative AI on HR—from recruitment and performance reviews to promotion decisions—as well as the potential implication of the then-proposed EU AI Regulation (AI Act).

Today, generative AI is no longer a future ambition. Multinational companies are rapidly deploying AI tools into daily business operations: from content creation and data analytics to automated decision-making. What was once a speculative legal concern has become a tangible compliance challenge, with the AI Act published in 2024 and its full application expected by August 2026.

As we move towards 2026, the real question is not *whether* to use AI, but *whether your people know how to use it*. Employers can no longer treat AI as a future topic: it is here, it is powerful, and more than ever it is accountable.

1. UNDERSTANDING THE RISKS

Companies are increasingly focusing on integrating the latest AI tools, but you do not need to be a specialist to know that deploying AI tools without properly equipping your employees to use them is a recipe for disaster: biased data leading to discrimination, privacy breaches, misinterpretation of AI outputs, and an overreliance on automation.

These risks can materialise in different ways, depending on the type of AI tool involved.

If **your company uses AI tools**, the risk lies in system configuration, how transparent they are, and whether employees understand how to use them responsibly.

On the other hand, **many employees now rely on tools like ChatGPT, Copilot, or Gemini** to perform their daily tasks. From drafting e-mail, brainstorming, summarising documents, and generating ideas to assisting with code, the increasing use of such tools comes with its own set of risks. Sensitive internal data may be inadvertently shared with third-party systems, outputs may contain factual errors or embedded biases, and copyright, confidentiality, or data privacy obligations may be unknowingly breached.

Whether the tool is company-provided or individually accessed, the common denominator is human behaviour. Without clear internal policies and proper awareness, even the most advanced systems can become sources of liability rather than innovation.

2. TRANSLATING AI RISKS INTO POLICY

Irrespective of the type of AI tools employees interact with, an internal AI policy is no longer optional. It is the most effective way to ensure regulatory alignment and minimise operational and reputational risks. An AI policy should:

§ Define acceptable use of AI tools (for both company-provided and third-party tools);

§ Establish how and when human oversight is required, particularly in high-impact decisions;

§ Set clear data boundaries, emphasising what can or cannot be entered into AI systems, especially confidential, intellectual property, and personal data;

§ Provide escalation channels for AI-related incidents;

§ Define relevant sanctions for infringing AI obligations;

§ Align AI policy with the obligations under the EU AI Act and relevant data protection laws.

More than a compliance document, a good AI policy gives employees clarity and transparency, while protecting employers against potential legal breaches, reputational damages, or third-party concerns.

3. TRAINING EMPLOYEES FOR THE AGE OF AI

Even the best policy is only as effective as the people expected to apply it. That is why employers must actively invest in building **AI literacy** across all levels of the organisation.

Whether they are working with AI tools made available by the company or using external chatbots, employees need to understand what data is safe to enter, how to critically assess AI-generated content, when human validation is needed, and how to report misuse or unexpected outcomes. Such training should be adapted based on the employee's role, technical expertise, as well as the context in which the tool is used.

AI training efforts should not be limited to IT or legal departments. AI awareness must become a core element of workplace culture.

4. THE SPECIAL CASE OF HR APPS WITH AI

While AI can bring efficiency, special attention should be given to AI systems used in employment-related decisions (e.g., recruitment, performance evaluation, promotion decisions, dismissal, etc.), as these are classified as high-risk systems under the AI Act. Such tools will only be permitted under strict conditions, including documentation, transparency, and human oversight. Emotion-recognition systems in the workplace, which attempt to infer mental states or emotions based on facial expressions or tone of voice, are explicitly prohibited.

In this context, HR professionals must play a central role. They should be involved not only in the implementation and use of AI systems, but also in internal governance.

5. YOUR CALL TO ACTION: WHAT EMPLOYER SHOULD DO NOW

With the full application of AI Act approaching, organisations should act proactively: identify AI systems currently in use, classify them based on risk, assess legal and operational risks, implement internal policies, and invest in role-specific training.

AI is transforming the workplace. The real measure of success will be how well companies understand, manage and communicate this change: not only at the top, but throughout the entire organisation. In this new landscape, each employee must be part of the solution.