



EU AI Act implications for US employers

Bloomberg Law

Written by Alice Wang, Deborah Margolis and Stephan Swinkels, Littler

The EU Artificial Intelligence Act, which is set to come into force shortly, is set to be the world's first comprehensive legal framework on AI. The new law will set a new standard for AI governance not only in the EU, but around the world—including for US employers. Here's what they should know.

Who Will the EU AI Act Apply to?

The responsibilities under the AI Act will fall on multiple different roles in the AI lifecycle, including providers (i.e., those who develop AI systems or put them on the market or into service) and deployers (i.e., those who use AI systems, which include employers).

The AI Act will apply to:

- Providers placing AI systems or generative AI models on the market in the EU, irrespective of where they are based; and
- Providers and deployers of AI systems that are based outside the EU, where the output produced by the AI system is used in the EU.

As such, the AI Act will be on many companies' geopolitical agendas, as despite being European legislation, it could potentially apply to companies that are not based or established in the EU. US companies may find themselves subject to the AI Act, even if they are not based in the EU if, for example, their AI systems or AI system outputs are used by EU customers or impact individuals in the EU.

What Does the EU AI Act Regulate?

The AI Act applies to a broad definition of AI and regulates both predictive AI (i.e., AI that leverages pattern recognition learned from historical data to make predictions when presented with new data) and generative AI (i.e., AI used to generate new outputs, usually in response to prompts, such as ChatGPT and other large language models). The AI Act takes a risk-based approach to the regulation of AI systems—the greater the potential risk that the AI poses to individuals, the greater the compliance obligations.

Unacceptable Risk

There is a prescribed list of AI practices that pose an “unacceptable risk” which will be banned under the AI Act. The focus is on AI systems that pose an unacceptable risk to people’s safety or are intrusive or discriminatory, and includes the use of AI systems to infer individuals’ emotions in the workplace (with limited exceptions).

High Risk

“High risk” AI systems under the AI Act will be subject to significant regulatory oversight, including systems used by employers:

- For recruitment or selection (in particular, for placing targeted job advertisements, analyzing and filtering applications, and evaluating candidates); and
- To make decisions affecting contract terms, promotions or terminations, allocating tasks based on individual behavior, personal traits or characteristics and monitoring employees’ performance and behavior.

This is likely to cover most uses made by employers of AI systems and, as a result, employers that use AI in the workplace will be required to take additional compliance steps, including (where they are providers):

- Developing the AI system to ensure it carries out the functions required under the AI Act (e.g., automatic record keeping and human oversight);
- Developing the AI system in accordance with specified governance procedures (e.g. risk management, quality management systems and testing);
- Preparing extensive evidence of compliance and technical documentation; and
- Other compliance requirements (e.g. affixing the CE marking of conformity and EU declaration of conformity, and registering on the EU database).

Where employers are deployers (for example because they are not developing their own AI systems), they will be subject to lesser obligations, many of which flow from the providers responsibilities, including:

- Informing individuals that they will be subject to the AI system before putting it into use;
- Ensuring that any AI system they use is compliant with the AI Act;
- Reviewing the suitability of input data;
- Completing risk assessments;
- Assigning human oversight to appropriate individuals;
- Using and monitoring the AI system in accordance with its instructions for use; and
- Retaining records produced by the AI system.

The penalties for non-compliance of the AI Act are very significant and can cost up to the higher of EUR 35 million (USD 38 million) or 7% of the company’s global annual turnover in the previous financial year. By way of comparison, this is almost double the maximum penalty for GDPR breaches (which itself was considered to be extremely high at the time that GDPR was implemented six years ago).

Next Steps

The majority of the AI Act’s provisions will apply two years after the AI Act enters into force—although the ban on unacceptable risk AI systems will apply after six months. In the meantime, US companies—both providers and deployers—should be conducting a thorough audit to understand whether they might fall within the scope of the AI Act and, if so, considering how their use or development of AI tools might be categorized under the AI Act and the associated compliance obligations.

US companies should prioritize evaluating whether any AI will be deemed to pose an “unacceptable risk” and ensure this is withdrawn ahead of the prohibition. US companies are advised to ensure that any new AI systems which are implemented have been developed with the upcoming legislation in mind and will enable employers to comply with their obligations. The consequences of non-compliance are steep, both in terms of monetary penalties and potential reputational harm. Finally, US employers should realize that the AI Act may very well serve as a model for more cohesive AI regulation in the US, which to date suffers from a fragmented regulatory framework.