Centrum für Europäische Politik
FREIBURG | BERLIN

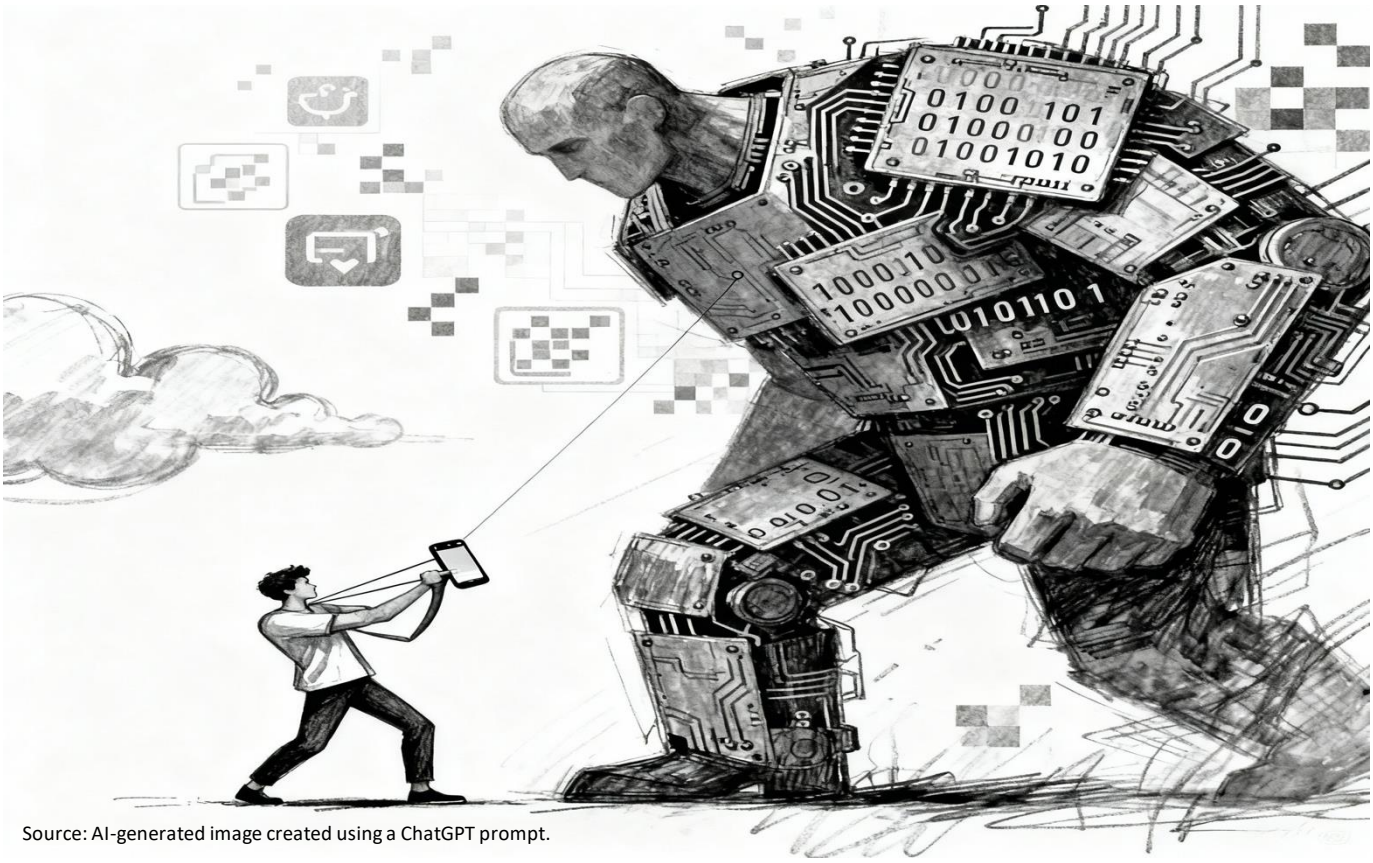
cepInput

No 17 | 2025 2 October 2025

SMEs Worldwide Must Prepare Now for Europe's New Ambitious AI Regulation

How to Turn Risks into Opportunities

Anselm Küsters and Ben Waber



Source: AI-generated image created using a ChatGPT prompt.

The European Union's AI Act aims to promote trustworthy Artificial Intelligence, but in doing so presents unique challenges for small and medium-sized enterprises (SMEs), especially those using AI for non-core functions. SMEs typically lack the resources to navigate complex compliance requirements, including conformity assessments, ongoing risk management, and bias detection. However, SMEs do not have to be passive rule-takers: By acting early, they can transform compliance into a competitive advantage. Three avenues stand out: building collective strength; adopting compliance-by-design; and exploiting sandboxes and SME derogations. As the Brussels effect is prompting non-EU buyers to demand "AI-Act-ready" assurances, SMEs that embrace these measures are more likely to secure future deals and partnerships.

This is a more detailed version of an article originally published in the Harvard Business Review under the title „How SMEs Can Prepare for the EU's AI Regulations" and accessible here: https://hbr.org/2025/09/how-smes-can-prepare-for-the-eus-ai-regulations?ab=HP-hero-latest-1.

Content

1 Introduction

Imagine you are the HR manager of a medium-sized manufacturing company with 250 employees spread across Europe and North America.[1] You receive hundreds of resumes for each job opening, often over 500 for a single position. Your small HR team cannot possibly review them all thoroughly, so you have implemented an in-house CV screening system powered by AI. This tool, based on a publicly available, open-weight large language model (LLM) and further trained on the resumes of past successful hires, helps identify promising candidates by assessing their skills, experience, and fit. One day, this AI tool identifies an exceptional candidate for a critical engineering role that you have been trying to fill. You are happy about this, but your elation is soon tempered by a sobering realization: this seemingly innocuous tool now places your company at the center of a regulatory conundrum.

Under the EU AI Act, which formally came into force on 1 August 2024 but features staggered compliance deadlines, this fictional CV screener is considered a "high-risk" application of AI. Other high-risk applications covered by the Act include AI systems evaluating creditworthiness for loans, AI managing critical railways or road infrastructure where failure could endanger lives, and educational AI systems used for determining access to education. All these high-risk applications of AI will be subject to strict compliance requirements starting on 2 August 2026. Companies that violate these rules could face significant fines of up to €15 million or 3% of their global annual revenue for most violations relating to high-risk systems (while non-compliance with the prohibition of AI systems, as listed in Art. 5, carries the highest penalties of up to €35 million or 7% of annual turnover). Suddenly, what were once simple efficiency tools have become potential liabilities.

It is not just large European companies that need to worry. The AI Act applies to companies of all sizes that develop, sell, or use any type of AI system in the European Union, or whose AI system outputs are used in the EU. Additionally, the General-Purpose AI Code of Practice, released in final form in July 2025, concretizes specific compliance obligations that apply based on computational thresholds rather than company size. What's more: Given the EU's regulatory influence, often referred to as the "Brussels effect," these rules are likely to shape AI governance globally. Tellingly, OpenAI recently sent a letter to Governor Newsom recommending that California treat developers of frontier models as compliant with state requirements "when they've signed onto a parallel framework such as the EU's AI Code of Practice". (As an aside, OpenAI likely did this to foreclose competition from startups.)

For small and medium-sized enterprises (SMEs), the challenges presented by the AI Act are particularly acute. While larger companies may have the resources to adapt and comply quickly, SMEs typically operate on tighter budgets and with smaller teams. For the same reasons, smaller firms may be more reliant on applications of AI in non-core business functions such as HR, including the aforementioned automated candidate screener as well as AI recruiting chatbots. Rather than developing such solutions from scratch or refining existing large language models, the new rules could prompt SMEs to outsource compliance and innovation to expensive intermediaries. Even worse, if companies do not want to burden themselves with funding an AI assurance firm or aim to avoid the legal uncertainty of in-house

[1] This is a more detailed version of an article originally published in the *Harvard Business Review* under the title „How SMEs Can Prepare for the EU's AI Regulations" and accessible here: https://hbr.org/2025/09/how-smes-can-prepare-for-the-eus-ai-regulations?ab=HP-hero-latest-1. We would like to thank Dr Thomas Clausen, Manager of Digital Policy at the German Electro and Digital Industry Association (ZVEI), for his helpful comments while preparing this article.

solutions, they might be incentivized to delay the implementation of AI tools, even if there would be productivity gains.

However, all is not lost. SMEs should act now to develop specific strategies to overcome these challenges, and they may even use compliance with the AI Act to set themselves apart from competitors who are less prepared.

2 Understand the (developing) regulatory environment

Most of the provisions for high-risk AI systems, including those used in HR, will go into effect on 2 August 2026, although the regulatory apparatus is already taking shape. The Act's enforcement follows a phased timeline: the prohibitions of certain AI systems came into effect in February 2025, and obligations for General-Purpose AI (GPAI) models came into effect in August 2025. After being delayed several times, a lengthy Code of Practice for GPAI models has now been published to help providers demonstrate compliance. The Code is organized into three chapters: Transparency, Copyright, and Safety & Security. The first two chapters apply to all GPAI providers, regardless of the model's potential impact. In practical terms, this means that every firm integrating a general-purpose AI model into their AI systems – whether a niche chatbot or a more general large model – must provide clear documentation and publish a summary of the training data to satisfy the requirements.

At this point, it helps to give some definitions: According to the AI Act, a GPAI model is defined as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks". The new guidelines argue that 10^{24} floating-point operations (FLOPS) of computing power are an "indicative criterion" for GPAI. Meanwhile, models exceeding 10^{25} FLOPS are presumed to pose "systemic risk", triggering additional duties such as adversarial testing, serious-incident reporting, and robust cybersecurity safeguards. Although the European Commission has repeatedly stated that its aim is to target only a small group of frontier developers, by June 2025, at least 33 publicly announced AI models from numerous developers had passed this threshold. As researchers have pointed out, AI rules that rely too heavily on computing power fail to recognize that the relationship between computing power and risk is highly uncertain and subject to rapid change.

For SMEs, the "downstream modifier" rule creates a critical compliance trigger that many may not anticipate. According to the relevant guidelines, if a company modifies an existing model – for example, by customizing a language model for HR screening – and the training compute used for the modifications exceeds one-third of that used for the original model, the company counts as a GPAI provider itself. These modifiers must then document changes, provide training-data summaries and, if the model is deemed to pose systemic risk, meet all the associated requirements.

However, the exact computation thresholds are still the subject of intense debate and are likely to change repeatedly in future. Moreover, the Commission acknowledged that it might postpone some AI Act obligations because the promised European harmonized standards are running late. In early July 2025, dozens of leading European companies publicly called on the Commission to "stop the clock" on the most stringent AI requirements. Moreover, the success of the GPAI Code depends on the AI Office's ability to drive implementation, which in turn is affected by several factors, ranging "from building up the AI Office's regulatory capacity, creating updating mechanisms for the [C]ode, to navigating a new geopolitical environment, not least by managing its relationship with the US' Center for AI Standards

and Innovation, whose explicit mission is to 'guard against burdensome and unnecessary regulation of American technologies'."

Given this volatile situation, SME leaders should plan as if the 2026 deadline is still in place, but maintain budget flexibility in case Brussels grants more time. More generally, they can be sure that the obligations for high-risk AI systems under the EU AI law will be quite extensive. Before an AI system can be marketed or used in the EU, its provider must undertake a rigorous conformity assessment to ensure that it meets a range of requirements, including those relating to data quality, transparency, human oversight, and cybersecurity. Significantly, internal production control can be used as a conformity assessment procedure. Later, a substantial modification means that it is essentially a new product, requiring another assessment round. Companies must also establish ongoing risk management systems to mitigate potential harm to users and data subjects. For example, the AI Act requires that our fictional CV screening tool must be trained on representative datasets and include bias detection systems. Previously, companies may have used readily available data sets without rigorous checks – especially if they designed their AI systems in-house. Now, they must actively curate diverse datasets and mitigate potential biases. This process is both technically challenging and resource-intensive.

Overall, leaders of SMEs should closely monitor official guidance and harmonized standards to stay abreast of the shifting regulatory environment. Alternatively, they could also look at ISO 42001, an international standard that specifies requirements for establishing an AI Management System within organizations. Still, much will depend on how the AI Act is implemented in practice in the coming months and years. The AI Act's reliance on the ambiguous concept of "intended purpose" illustrates this problem, as general-purpose AI systems like ChatGPT often lack a single, predefined use. With its overly complex and ambiguous requirements, the EU AI Act might disadvantage smaller players who lack the resources to interpret and implement them effectively.

3 Understand exposure and compliance costs

As the effective application date of the EU AI Act approaches, affected companies must nevertheless clear several hurdles: To begin with, they should conduct a comprehensive inventory of all AI systems in use, cataloguing each system's functionality, the underlying models and data sources used, the deployment context, and the company's role as provider, deployer, importer, or distributor. Most importantly, they must then assess each system rigorously against the EU AI Act's risk classification criteria to determine whether it is high-risk. According to Art. 6(1) of the EU AI Act, an AI system shall be considered high-risk if it is intended to be used as a safety component of a product covered by Union harmonization legislation listed in Annex I *and* if the product is required to undergo a third-party conformity assessment. Tellingly, however, the Commission guidelines on classifying high-risk AI systems, and related requirements and obligations, are not yet available (as of writing, the target date appears to be February 2026).

For those AI systems classified as high-risk, such as our HR tool, providers must implement and maintain an iterative risk-management system. This system must span the entire AI lifecycle in order to identify, evaluate, mitigate, and monitor foreseeable harms, ranging from algorithmic bias and safety vulnerabilities to data protection and cybersecurity threats. At the same time, providers must establish a documented quality management system. This system must include written policies, development and testing procedures, and change management controls to ensure consistent compliance and traceability. Providers must also guarantee transparency and human oversight, disclosing when and how AI

is used, and embedding mechanisms that allow trained personnel to halt AI-driven decisions when necessary. Furthermore, documentation detailing the system's purpose, architecture, data governance practices, performance metrics, and the results of conformity assessments must be drawn up before market placement – and later be kept up to date. Finally, before marketing any high-risk AI system in the EU, providers must register it in an EU database.

Taken together, this complex and developing regulatory environment for AI poses challenges for businesses, in particular SMEs. In his popular report on EU competitiveness, Mario Draghi argues that the EU's regulatory burden challenges, above all, SMEs in digital sectors, with more than half of SMEs in Europe citing regulatory barriers and administrative burdens as their largest problem. With respect to the AI Act, researchers estimated that setting up the quality management system mentioned above costs €193,000–330,000 initially and approximately €71,400 annually to maintain. For SMEs that cannot develop their own large models from scratch, the gradual transition from deployer to (compliance-heavy) provider through modifications such as fine-tuning, Retrieval-Augmented Generation, and the inclusion of meta-prompts is problematic. According to a survey by Deloitte Germany, 52 percent of respondents are concerned that the AI Act will limit their opportunities for AI innovation, and only 36 percent say their organizations are well-prepared to implement the law.

To a large degree, this negative outlook for businesses is driven by legal uncertainty. For instance, several stakeholder consultations and surveys have voiced concerns about the clarity and scope of the definition of "AI system" in the EU AI Act. The Commission's own guidelines, published in February 2025, suggest ongoing ambiguity around key concepts, with the industry being unsure what constitutes "manipulation" and "significant harm" in AI systems. A particular concern for industrial companies is how the AI Act interacts with existing product safety regulations. Industry representatives argue that the Act introduces problematic duplication of regulation, given that existing product safety laws already cover AI-enabled products – for instance, the new Machinery Regulation already incorporates self-evolving behavior. With the August 2026 deadline approaching, SME leaders must make a strategic decision: either delay the adoption of AI, given this complexity and uncertainty – or transform compliance into a competitive advantage.

4 Prepare to win on AI compliance

While ambiguous regulation and heavy compliance costs typically entrenches incumbents, SMEs are not powerless. A recent interview-based study found that SMEs demonstrate greater agility and flexibility in AI adoption than large corporations. Leveraging this strength, a comprehensive AI Act action plan for SMEs involves building strategic partnerships, implementing compliance-by-design, and turning compliance into a competitive and marketing advantage.

1. Strategic partnerships

AI Act compliance costs can be material for SMEs – one widely used model estimates 17.3% of total revenues – making cost-sharing essential. A strategic AI adoption framework for SMEs therefore emphasizes that internal and external collaboration, e.g. through organizing workshops and sharing success stories and case studies, allows for knowledge sharing and ensures that SMEs stay informed. If implemented through the correct channels, these practical measures do not violate antitrust law's anti-collusion rules. The AI Act explicitly requires Member States to provide SMEs with dedicated communication channels for guidance and queries, proportional conformity assessment fees, and support

for participation in standardization. SMEs could expand upon these strategies: For example, an SME consortium could conduct joint bias and robustness testing using common tools and then produce its own technical file to support conformity assessment. This would reduce the cost and time per firm while probably also increasing regulator confidence in the chosen tools.

SMEs can pursue AI partnerships through horizontal collaboration with peers and vertical partnerships with specialized service providers. One emerging real-world example is Saidot, an AI governance startup based in Helsinki that secured €1.75 million in seed funding after developing compliance solutions to help organizations align with the requirements of the EU AI Act. This attracted clients including the Scottish Government and Deloitte. Similarly, Silo AI – Europe's largest private AI lab, founded in Helsinki in 2017 – has leveraged its expertise in responsible AI development and open-source multilingual models to attract major enterprise clients. This ultimately led to its €615 million acquisition by AMD. Another notable case is that of AIcendence, a German healthcare AI startup that successfully navigated complex rules by collaborating with the European Digital Innovation Hub (EDIH) Schleswig-Holstein. This enabled the rapid development of an AI-powered diagnostic tool and secured them government funding.

2. Compliance-by-design

If SMEs are developing AI systems in-house, they should incorporate compliance features from the outset rather than adding them later. Tellingly, AI compliance experts argue that building compliance features from the outset is more cost-effective, with companies achieving savings of $3.05 million per data breach through proactive compliance measures. Intuitively, it is easier and cheaper to document everything from the start than to reconstruct compliance trails later. Accordingly, SMEs should start by mapping their data-driven use cases to the risk tiers of the AI Act, establishing a quality management system as quickly as possible, and recording accuracy, robustness, and biases, using publicly available benchmarks. This will actually help them to improve their AI-based products and services over the medium term by highlighting any problems in the training data and indicating which automated steps should be accompanied by human oversight (known as "human-in-the-loop" decisions). For example, when SMEs customize HR models, any biases compound quickly: Biased training data and algorithms create discrimination that violates the law and reduces the effectiveness of talent acquisition, as biased AI systems miss qualified candidates and damage the employer brand.

Crucially, the AI Act stipulates that SMEs should have priority access to "regulatory sandboxes", free of charge, enabling and formalizing such compliance-by-design testing. Sandboxes are designed to involve standards organizations, EDIHs, testing facilities, and other actors – so SMEs should engage these partners early to co-develop test plans and align with emerging standards. Each EU Member State must establish at least one AI regulatory sandbox by August 2, 2026, and documentation from sandbox participation can be reused to demonstrate compliance; firms are protected from administrative fines when acting in good faith under sandbox guidance. Evidence from the Financial Conduct Authority's regulatory sandbox in the UK suggests significant benefits, including a 15% increase in capital raised by participating firms and a 50% higher probability of securing funding. The program has achieved lasting effects, with 90% of firms from the first cohort progressing to market launch. Arguably, the regulatory sandboxes under the AI Act could look very differently. Still, supervised testing in AI Act-related sandboxes promises to reduce regulatory uncertainty and signal quality to investors and enterprise buyers. The EUSAiR project, which is funded by the European Commission, aims to facilitate access to AI regulatory sandboxes for SMEs and start-ups, thereby helping them to reduce compliance costs.

3. Compliance-to-advantage

Finally, there is evidence that ethical AI adoption can help small businesses build more trust among customers and partners – which is urgently needed. Over the past five years, global consumer trust in AI has fallen from 61% to 53%, with a particularly sharp decline in the US. A systematic literature review shows that algorithmic discrimination and bias hinder trust in AI, whereas perceived fairness or justice enhance it. When AI systems exhibit errors, "hallucinations", or biases, the foundation of trust between organizations and their stakeholders is directly undermined. Even worse, "the faulty decisions that result most often impact multiple stakeholder groups", as explained by Deloitte researchers. This is crucial to understand for SMEs, which often depend on close-knit relationships with long-standing suppliers and customers, and should therefore prioritize ethical AI adoption.

If everyone must comply, how can an SME stand out? While basic compliance creates a level playing field, it is early adoption, transparency, and targeted marketing that help create differentiation. Once the current "hype phase" of generative AI inevitably fades, SMEs with working products and services whose capabilities are rigorously documented can transform their compliance outputs into customer-facing assurances, showcasing transparency to speed up the procurement process. For example, publishing "model cards" – standardized documentation frameworks popularized on platforms such as GitHub and Hugging Face – provides structured transparency regarding the capabilities and limitations of AI systems, and makes this information easily accessible to a range of stakeholders. Research shows that adding detailed model cards to previously undocumented models correlates with increased download rates. Further visible signals could include participating in the aforementioned sandboxes and proactively obtaining external conformity assessments. In general, the first-mover advantage in AI compliance is particularly significant, given that the EU was the first jurisdiction to establish comprehensive AI regulation. Firms with relevant expertise could contribute to the development of harmonized standards (such as those currently being developed in CEN/CENELEC JTC21), which can then be used to demonstrate compliance with the AI Act.

5 Conclusion

One of the biggest unintended risks of the EU AI Act is that it could entrench the current market leaders and hinder innovation by imposing real or perceived compliance obligations that would disproportionately affect smaller companies. However, the idea that only Big Tech can survive is exaggerated. The Act itself contains numerous SME-friendly measures, such as priority access to regulatory sandboxes, ready-to-use templates, dedicated guidance channels, and targeted training. Furthermore, most AI projects will not exceed the compute-intensive thresholds that trigger heavier rules, even when fine-tuning models.

Unlike large incumbents, who are weighed down by legacy systems and layers of approval, SMEs can adapt workflows much easier – and thus gain competitiveness. For instance, integrating compliance features into the AI development lifecycle from the outset, i.e. mapping use cases to AI Act risk tiers, implementing quality management systems, and monitoring accuracy, robustness, and bias metrics, prevents the need for costly revisions. Human-in-the-loop safeguards and proactive documentation such as model cards satisfy regulators and surface data issues early on, thereby improving product performance and reducing breach and liability risks. Furthermore, SMEs can dramatically reduce costs per firm and accelerate market entry by forming consortia, co-developing bias and robustness tests, and sharing assessment experiences. Similarly, priority sandbox access and EDIHs distribute the burden

across partners and boost regulator certainty. Finally, ethical AI can be a market differentiator when the hype fades. Early adopters of transparent practices, such as publishing auditable incident logs, bias dashboards, and open model cards, might gain first-mover status in procurement and investment rounds.

To unlock this potential, Europe must do its part, too. Regulators should keep SME templates up to date and streamline overlapping data-protection rules, e.g. by looking at the overlap between the Fundamental Rights Impact Assessment and the Data Protection Impact Assessment. They should also underwrite open-source compliance tooling and support SMEs without the manpower to participate in standard-setting meetings to enable them to participate in the standardization process. One way to achieve this would be through Small Business Standards, a European non-profit association established with the support of the Commission. If both sides deliver, Europe's high-stakes approach to AI need not pose a high risk to its innovators.

Centrum für Europäische Politik
FREIBURG | BERLIN

Authors:

Dr. Anselm Küsters, LL.M., Head of the Department of Digitalisation/New Technologies
kuesters@cep.eu

Ben Waber, PhD., Visiting scientist at MIT and Senior Visiting Researcher at Ritsumeikan University
ben.wbr20@gmail.com

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4205 | D-10117 Berlin
Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS, and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Free of vested interests and party-politically neutral, the Centres for European Policy Network provides analysis and evaluation of European Union policy, aimed at supporting European integration and upholding the principles of a free-market economic system.