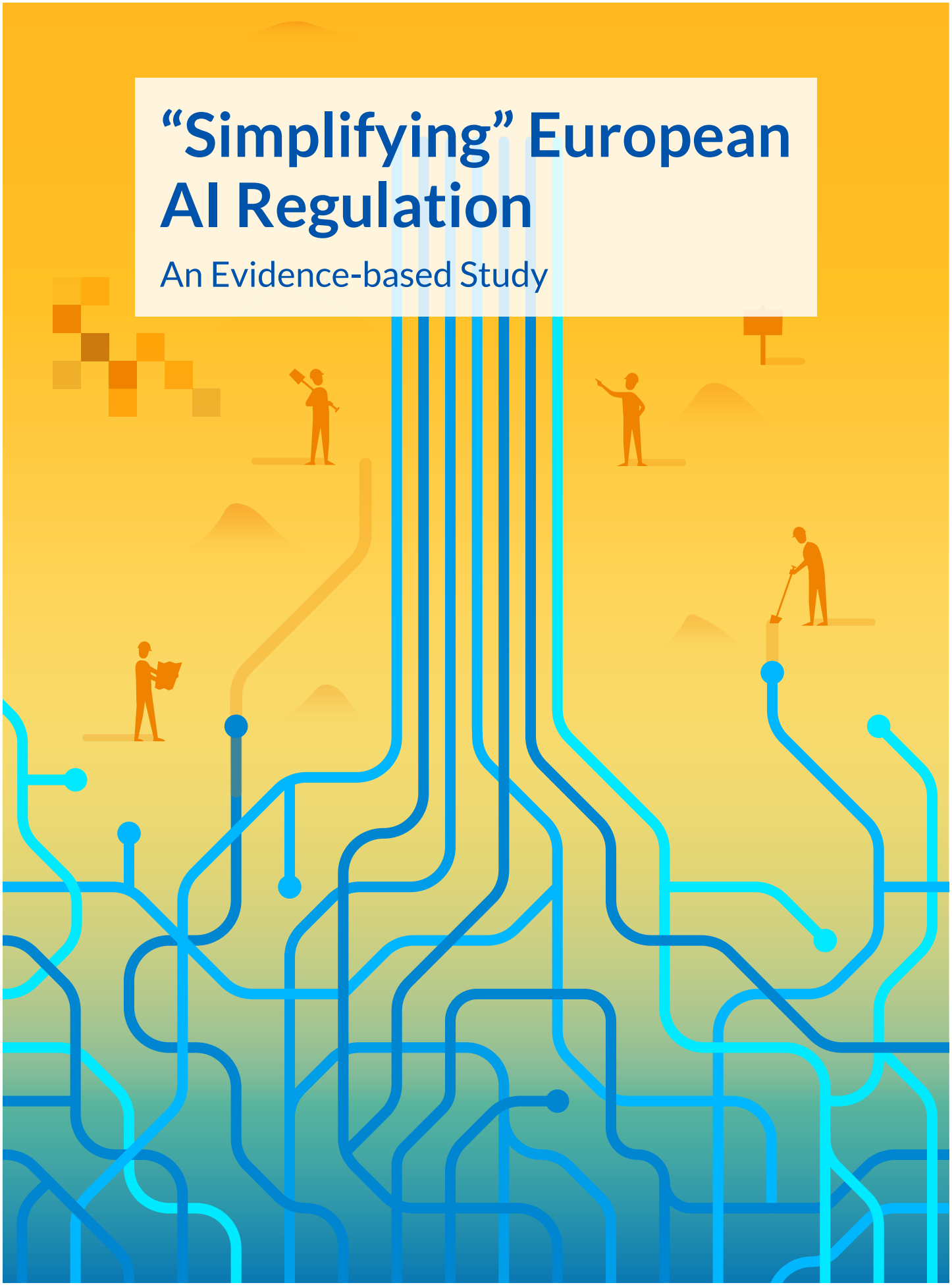
# “Simplifying” European AI Regulation

## An Evidence-based Study



Supported by

GERMAN AI ASSOCIATION

Commissioned by

BertelsmannStiftung

## Commissioned by


November 2025

**Publisher**
Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Phone +49 5241 81-0
www.bertelsmann-stiftung.de

**Supported by**
German AI Association

**Responsible for content**
Asena Soydaş
Project Manager
Programme Digitalization and the Common Good
Phone +49 5241 81-81247
asena.soydas@bertelsmann-stiftung.de

**Layout**
Nicole Meyerholz, Bielefeld

**Editing**
Barbara Serfozo, Berlin

**Image Credits**
© Paul Feldkamp



**10.11586/2025099**

**Recommended citation style**
Hacker, P., Kilian, R. & Costas, J. (2025) Simplifying European AI Regulation - An Evidence-based Study. Gütersloh: Bertelsmann Stiftung.

# “Simplifying” European AI Regulation

## An Evidence-based Study

**Prof. Dr. Philipp Hacker & Dr. Robert Kilian (Law & Policy)**
**Prof. Dr. Jana Costas (Empirical findings)**

BertelsmannStiftung

# Contents

# Preface

In August 2024, the AI Act entered into force as one of the European Union's most recent digital regulatory frameworks and has since been moving step by step into its implementation phase. Yet even before the first provisions take full effect, it is becoming clear that implementation in practice faces significant hurdles. The development of key standards, technical guidelines, and cross-sectoral interpretations needed for consistent application is progressing slowly. In many member states, the establishment of national enforcement authorities is delayed, and coordination between national and European levels remains unclear in several areas. These practical challenges not only jeopardize smooth implementation but also risk fragmentation and inconsistency within the European legal space.

At the same time, the debate on the future of European competitiveness and regulation took on a new political dimension with the publication of the Draghi Report in September 2024. Mario Draghi emphasizes that Europe's economic strength depends on how effectively innovation and regulation are aligned. His main objective is to streamline and harmonize existing legal frameworks to create the foundation for sustainable competitiveness. A year later, in his reflections on the Draghi Report, he highlighted the growing strategic importance of digital regulation and artificial intelligence, while also pointing to persistent barriers in implementation and enforcement, and to the need for more practical and effective approaches. This debate has also gained urgency with a view across the Atlantic and beyond, amid rising geopolitical pressure on Europe to safeguard its digital and economic sovereignty. With this, the discussion surrounding the AI Act and other digital laws is once again not merely technical or legal but highly political, touching on the core questions of Europe's economic, technological, and democratic future.

With the Omnibus Agenda, the European Commission is now seeking to respond to these challenges. The initiative spans six thematic packages, ranging from sustainability and investment to agriculture, security, and industry, and aims to modernize the European legal framework by 2030, reduce bureaucracy, and eliminate contradictions between existing regulations. The Digital Package, forming part of Omnibus IV within this agenda, focuses specifically on simplifying existing digital acts. The goal is to avoid overlaps and redundancies, harmonize reporting requirements, and make the regulatory framework more practical. For the first time, key digital laws are being jointly reviewed for coherence, clarity, and applicability.

Our new study, ***"Simplifying" European AI Regulation – An Evidence-based Study***, examines what opportunities the AI Act itself offers for simplification and how these could be implemented in practice. Based on 15 semi-structured interviews and a stakeholder workshop with companies, startups, associations, and civil society organizations from across Europe, the study analyzes where the main practical and structural hurdles lie and formulates proposed actions for achieving simplification, coherence, and legal certainty without weakening the protective purpose of the law.

The authors make clear that simplification does not mean deregulation but rather more precise regulation, with clear responsibilities, comprehensible requirements, and consistent procedures that strengthen trust, efficiency, and competitiveness alike.

Our study comes at a decisive moment. On November 19, 2025, the European Commission published its Digital Omnibus Regulation Proposal as part of the broader Digital Package, which includes the AI Act, the Data Act, the General Data Protection Regulation (GDPR), and cybersecurity directives such as NIS2. The proposal lays the groundwork for the negotiations that are now under way. The European Union is at a stage where the guardrails of digital policy are being redrawn and where it will be decided whether regulation can be simplified without losing clarity, protection, and value orientation.

What is decided in the upcoming negotiations on the Digital Omnibus Regulation and how it is decided deserves close attention. Simplification must not turn into a political measure that ultimately weakens trust and institutional structures rather than strengthening them. It requires clear, fair, and practicable rules that give European start-ups and SMEs guidance while at the same time safeguarding our fundamental and digital freedoms and preserving the core of the existing European digital regulatory framework, which is founded on transparency, fairness, and democratic participation. These foundations must not be lightly put at risk amid the Digital Omnibus discussions.

We thank the authors Prof. Dr. Philipp Hacker, Dr. Robert Kilian, and Prof. Dr. Jana Costas for their important contribution to the European debate on AI regulation, and the German AI Association for its constructive support and for opening its networks.

Our gratitude also goes to all interview partners and participants in the joint workshop from civil society, business, and academia, whose perspectives have contributed to a multifaceted and nuanced discussion.

We welcome feedback and ideas on this publication and, above all, look forward to continuing the exchange on responsible advancement of European AI and digital regulation.

Asena Soydaş
Project Manager
Program on Digitalization and the Common Good
Bertelsmann Stiftung

# List of Abbreviations

| | |
|---|---|
| AIA | Artificial Intelligence Act |
| BLEU | Bilingual Evaluation Understudy |
| CEN | European Committee for Standardization |
| CENELEC | European Committee for Electrotechnical Standardization |
| CJEU | Court of Justice of the European Union |
| CRR | Capital Requirements Regulation |
| DMA | Digital Markets Act |
| DSA | Digital Services Act |
| FLOP | floating point operations |
| FRIA | Fundamental rights impact assessment |
| GDPR | General Data Protection Regulatio |
| GPAI | Global Partnership on Artificial Intelligence |
| KYB | Know Your Business |
| LED | Law Enforcement Directive |
| LLM | large language models |
| MDD | Medical Devices Directive |
| MDR | Medical Devices Regulation |
| MDR | Medical Device Regulation |
| MR | Machinery Regulation |
| NLF | New Legislative Framework |
| OJEU | Official Journal of the European Union |
| PLD | Product Liability Directive |
| PWD | Platform Work Directive |
| RBI | Remote biometric identification |
| SME | Small and midsize enterprises |

# Executive Summary

This report presents an evidence-based analysis of how the European Union can streamline and strengthen its AI regulatory framework without undermining its commitment to fundamental rights. Rooted in qualitative research – including interviews and a focus group workshop with leading European AI providers, deployers and civil society organizations – the study identifies key challenges in implementing the EU AI Act and proposes concrete, rights-preserving actions that enhance clarity, feasibility and competitiveness.

The study interprets "simplification" not as deregulation but as clarification and disentanglement. Its aim is to reduce overlapping obligations, align horizontal and sector-specific rules and ensure consistent enforcement while maintaining accountability, transparency and proportionality. The findings show broad stakeholder support for the AI Act's objectives but also significant concerns about fragmented regulatory regimes, vague definitions, disproportionate burdens on smaller firms and institutional delays that impede effective compliance.

Companies generally support the Act's risk-based approach but struggle to apply it in practice, particularly with high-risk classifications, documentation requirements and assigning responsibilities across the AI value chain. Civil society organizations defend the Act's normative foundation and warn that any "simplification" must not erode rights protections, especially in areas such as biometric surveillance and algorithmic accountability. Both groups call for timely guidance, harmonized standards and structured institutional support to make compliance workable.

Building on these insights, the report formulates nine policy areas for targeted reform. The recommendations fall into three overarching vectors:

1. Refining risk classification and governance – enabling sector-specific regulation to guide high-risk oversight, eliminating duplicative procedures, and clarifying obligations for general-purpose and fine-tuned AI models.

2. Recalibrating technical and procedural requirements – replacing rigid or redundant provisions with performance-based criteria, proportional documentation duties and clearer definitions aligned across EU legislation.

3. Strengthening accountability and institutional coherence – defining liability throughout the AI value chain, establishing unified oversight structures, and providing sustained financial and technical support for SMEs and civil society organizations.

The proposals are organized by implementation horizon (see Table 1 p. 61. ***Short-term actions*** prioritize immediate technical clarifications, removal of duplicative requirements, adjustments to enforcement deadlines, and improved guidance and support for small and midsize enterprises (SMEs). ***Medium-term measures*** focus on building institutional capacity, harmonizing standards and developing a dedicated employment-related AI instrument under Article 153 of the Treaty on the Functioning of the European Union. ***Long-term reforms*** call for stable funding

mechanisms for SME and civil society (CSO) engagement and a robust enforcement architecture for general-purpose AI.

Policymakers can use this roadmap to sequence interventions that protect fundamental rights, ensure market functionality and support innovation ecosystems, particularly for smaller SMEs.

The report concludes that meaningful simplification requires legal precision, regulatory coordination and practical support – not a weakening of safeguards. The future of European AI governance depends on striking a balance between competitiveness and rights protection,[1] ensuring that simplification enhances coherence and accountability while upholding the European Union's constitutional and democratic commitments.

1 We gratefully acknowledge the excellent research support provided by Lilo Meier and Jakob Riediger.

# I. Introduction

For the EU, the past decade has been defined by an ambitious wave of digital regulation. While this effort has delivered essential protections against online harms (Digital Services Act, DSA), anti-competitive behavior (Digital Markets Act, DMA), and unchecked processing of personal data ( General Data Protection Regulation, GDPR), it has also produced a dense web of overlapping, intertwined and sometimes contradictory acts and rules that have become increasingly difficult to navigate.

Spurred in part by a renewed focus on competitiveness following the Draghi report, the European Commission has launched an initiative to "simplify" EU digital regulation. In our view, simplification should be understood as clarification – closing loopholes and untangling regulatory overlaps – rather than deregulation. Yet what has been missing from the debate is an empirically grounded assessment of feasible amendments to the digital acquis. Building on our recent white paper, this study aims to fill that gap by outlining ways to streamline AI regulation without compromising the EU's commitment to fundamental rights.

Our analysis identifies specific areas where regulatory overlap creates unnecessary burdens, where sector-specific expertise could better address AI risks and where technical requirements fail to align with operational realities. The study draws on semi-structured interviews and a focus group with leading European companies – both AI providers and deployers – as well as civil society organizations to develop recommendations that strengthen the EU AI Act with a dual objective: enhancing competitiveness while safeguarding fundamental rights.

Our empirical research shows that stakeholders broadly support the objectives of the EU AI Act. They recognize its potential to establish a trustworthy governance framework and prevent misuse. But companies, in particular, raise concerns about practical implementation – the need for regulatory clarity, the risk of excessive administrative burdens and the importance of coordinated guidance and technical standards. Key priorities include streamlining horizontal and sector-specific requirements, ensuring coherence across the wider EU digital regulatory landscape and clarifying responsibilities along the AI value chain. Civil society organizations, while even more supportive of the Act's overarching ambition, warn against attempts to dilute or reopen its provisions. They call instead for stronger transparency rules, consistent accountability mechanisms and the closure of loopholes, especially in sensitive areas such as biometric surveillance. While corporate actors emphasize feasibility and operational practicality, civil society groups focus on democratic oversight and the protection of fundamental rights. Despite these different perspectives, there is widespread agreement that the Act's success will depend on detailed guidance, strong institutional support and the effective translation of legal principles into practice.

Drawing on our empirical findings, our proposals target three broad dimensions of AI Act reform. First, we examine the classification and regulation of high-risk AI systems, particularly in areas where existing sectoral frameworks already provide extensive oversight. Second, we address technical requirements that create implementation challenges without delivering meaningful safety benefits. Third, we outline mecha-

nisms to clarify liability and responsibility across the AI value chain, especially for modified general-purpose AI models.

The remainder of this study is structured as follows. Section II presents the results of our empirical research, detailing stakeholder views on the Act, practical and substantive critiques, anticipated implications and recommended actions. Section III outlines our core policy proposals, organized into nine areas: prohibitions; high-risk provider obligations under Articles 6–24; high-risk deployer obligations under Articles 26–27; general-purpose AI provider requirements; value chain responsibilities; general obligations; technical standards; implementation deadlines; and SME exemptions and support. Each subsection offers targeted amendments to address specific regulatory inefficiencies identified in our research. Section IV concludes with reflections on the balance between "simplification" and rights protection.

# II. Empirical findings

The findings presented here draw on semi-structured interviews and a focus group with key stakeholders involved in, or affected by, the implementation of the EU AI Act. The interviews were designed to capture a wide range of perspectives on the Act's opportunities, challenges and practical implications. Through qualitative analysis, several overarching themes emerged – from broad support for the Act's objectives to concerns about day-to-day implementation and proposals for improvement.

Terminology follows the AI Act's definitions where applicable. "Providers" refers to entities that develop or place AI systems on the market; "deployers" to entities that use such systems in practice; "general-purpose AI (GPAI)" designates models adaptable across multiple contexts; and "high-risk" refers to systems covered by the Act's risk taxonomy. Several stakeholders, however, questioned the stability of fixed risk categories, noting that many harms are context dependent.

## A. Methods

In order to elicit diverse perspectives on the European AI Act, the empirical study followed a qualitative research design comprising 15 semi-structured interviews conducted between September and October 2025, as well as a hybrid focus group workshop with 15 diverse stakeholders held in October 2025. This approach allowed for systematic data collection on predefined themes while leaving room for new insights to emerge. A purposive sampling strategy ensured representation of stakeholders with distinct backgrounds, including civil society organizations and private companies ranging from small and mid-size enterprises to large firms. Participants were active in sectors such as banking, healthcare, manufacturing, technology, legal services and automotive, at the German, European and global levels. The companies represented both deployers and providers of AI systems, including those developing or working with general-purpose AI and high-risk AI systems.

The interviews were conducted via Zoom and lasted between 38 and 55 minutes; one participant provided written responses. In some cases, multiple interviewees joined the same session. Interviews were held in either English or German. To structure the discussions and contextualize the data, interview guides and organization-specific dossiers were prepared in advance, drawing on document analyses of websites, press releases and position papers. The guides focused on how different stakeholders perceive and evaluate the EU AI Act and its implications. With participants' consent, all interviews were recorded, transcribed and anonymized. Before each interview, participants were informed that the study was part of a research project funded by the Bertelsmann Stiftung.

The data were analyzed in MAXQDA by two researchers using an inductive approach that allows concepts to emerge from the material rather than from predefined theories (Gioia, 2021). This method is well suited to studying complex and evolving phenomena such as artificial intelligence and its regulation. Coding proceeded iteratively in three stages: open coding to identify first-order concepts; axial coding to group these into second-order categories; and selec-

Figure 1 | **Data Structure**

| 1st Order Categories | 2nd Order Themes | Aggregate Dimensions |
|---|---|---|
| · Reliable, Trustworthy Standard<br>· EU-wide Regulation instead of National Approaches<br>· Guiding Innovation<br>· Fighting Manipulation, Bias and Misuse | **Welcoming Attitudes** | **1.** General Climate |
| · Fundamental Opposition<br>· Critique of the Legislative Process<br>· Calls for Adjustment and Concrete Measures | **Critical Attitudes toward the AI Act** | |
| · Learning and Internal Capacity Building<br>· Integration into Existing Processes | **Preparedness** | **2.** Status Quo Implementation |
| · Atmosphere of Uncertainty and Fear<br>· Timeline Constraints<br>· Operational and Resource Challenges<br>· Lack of Contact Points, Guidance or Institutional Support | **Obstacles** | |
| · Multiple Regulatory Layers<br>· Redundant Documentation and Reporting Obligations<br>· Conflicting Definitions and Requirements<br>· Fragmented Institutional Responsibilities and Lack of Coordination | **Lack of Harmonization** | **3.** Substantive Critique |
| · Inconsistent/Overlapping Horizontal and Vertical Requirements<br>· Comprehensive Existent Risk Management Standards<br>· Capacity Constraints and Administrative Burden for Notified Bodies | **Tension Horizontal/ Vertical Regulation** | |
| · General Support<br>· Context Dependency of Risk<br>· Practical Uncertainty and Burden of Classification<br>· Risk of Loopholes and Misclassification | **Risk-Based Classification Logic** | |
| · Unclear Responsibilities and Responsibility Gaps<br>· Transfer of Liability<br>· Open-Source Paradox | **Value Chain Challenges** | |
| · Excessive and Redundant Documentation Requirements<br>· High Compliance Costs and Resource Constraints | **Documentation Obligation** | |
| · Global Regulatory Differences<br>· Loss of European Competitiveness and Sovereignty<br>· Dependence on Large Providers | **Global Competitiveness** | **4.** Implications |
| · Avoidance of AI or High-Risk Products<br>· Longer Development Timelines<br>· Investor Skepticism | **Slowdown in AI Development/Adoption** | |
| · Vague Compliance<br>· Calculated Non-Compliance<br>· Positioning to Minimize Regulatory Exposure | **Strategic Adaptations and Market Shifts** | |
| · Disproportionate Burden on SMEs<br>· Compliance as Competitive Advantage | **Asymmetries and Unequal Conditions** | |

| 1st Order Categories | 2nd Order Themes | Aggregate Dimensions |
|---|---|---|
| · Standards, Clear Guidance and Guidelines<br>· Central Point of Contact<br>· Support for SMEs<br>· Extension of Implementation Period<br>· Regulatory Sandboxes | **Implementation Support and Timeline** | **5. Proposed Actions** |
| · Regulatory Mapping<br>· Cross-Regulatory Synergies | **Simplification and Harmonization** | |
| · Dynamic Legal Development<br>· Stronger Involvement of Stakeholder Interests (CSOs/ Industry)<br>· Merely Voluntary Compliance Combined with Self-Assessment | **Regulatory Process Design** | |
| · More Fine-grained Risk Classification<br>· Clarification of Responsibilities along the Value Chain<br>· Certificate-Based Approach<br>· Consistent Transparency Obligations<br>· Safeguards for Fundamental Rights | **Refinement and Strengthening** | |

Source: own illustration

BertelsmannStiftung

tive coding to abstract them into aggregated dimensions (Corbin & Strauss, 2015). Analytical quality was ensured through peer briefings, intercoder reliability checks and member validation (Lincoln & Guba, 1985).

The following section presents the results in accordance with the resulting data structure (see graph below). Consistent with qualitative research standards, reflexivity was maintained through multi-voicing practices to reflect the diversity of stakeholder perspectives (Alvesson et al., 2008). Some quotations were translated from German into English and lightly edited for clarity. Informed consent was obtained from all interviewees for the inclusion of their quotations in this publication.

## B. Findings

This section presents stakeholder perspectives on the EU AI Act, with a focus on implementation challenges, governance gaps and proposals for refinement. It highlights broad support for the Act's objectives, alongside persistent uncertainty about its practical application. Key themes include overlapping regulatory requirements, unclear accountability structures and disproportionate burdens on smaller firms. The findings show how these challenges influence adoption strategies, competitiveness and compliance, and they outline proposed adjustments aimed at clearer guidance, phased enforcement and stronger coordination to keep the Act both workable and protective.

Aligned with the study's data structure, the section is organized into four parts. Section 1 describes the Status Quo, capturing a general climate of cautious endorsement coupled with practical obstacles that organizations face. Section 2 presents the Substantive Critiques raised during the interviews. Section 3 examines anticipated Implications for innovation practices, market dynamics and European competitiveness. Section 4 outlines the Proposed Actions, including considerations related to timelines, guidance, simplification, harmonization and regulatory refinement.

## 1. Status quo

The overall climate surrounding the EU AI Act is marked by cautious optimism. Across interviews and stakeholder groups, the regulation is generally viewed positively and is widely seen as a necessary step toward establishing a coherent framework for AI governance in Europe.

> *"Generally speaking, we welcome regulation that promotes the development of reliable and non-discriminatory AI systems. Moderate regulation is definitely a good thing." (Maria Zerhusen, Head of Research, Empion GmbH)*

> *"We also, of course, welcome the European Commission's proposal to create a trustworthy AI ecosystem." (BMW Group)*

> *"The AI Act provides a risk-based framework with clear definitions that ensure legal certainty and consumer trust, both of which are essential for the market to thrive and SMEs to innovate." (European DIGITAL SME Alliance)*

> *"It's a democratic achievement that we have this AI regulation – it allows us to counter the technological power that holds sway over our society." (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie)*

Companies view the Act as the first major attempt to set global standards for the ethical and responsible development of AI, positioning the EU as a normative leader in a rapidly evolving policy field. Although the tone of support varies – from pragmatic approval among corporate actors to more cautious endorsement from civil society organizations – the Act serves as a common point of reference in an otherwise fragmented debate on AI regulation.

> *"[W]e understand that there is a big political appetite to regulate AI technology because it obviously has dangers embedded. So, if we need to regulate it, we do prefer one regulation within the EU because as a multinational company, it's easier for us to comply with one act than 27. Because when we compare what's happening in the U.S. and each state is looking into AI in their own way, we do prefer a European approach." (SAP)*

Interviewees also emphasize that a unified European framework can help ensure fair competition across sectors and Member States while strengthening public trust. Several interviewees describe the Act as an enabler rather than a constraint – a tool that offers guidance and regulatory clarity while helping reduce risks related to manipulation, bias, misuse and abuse.

> *"It doesn't just hinder innovation – it also steers it. When the state, or in this case the EU, sets out which kinds of innovation it wants and which it doesn't – for example, through these prohibitions that essentially say: we don't need any new startups in these areas because these are systems we don't even want to use – then that also directs innovation." (CSO)*

> *"[W]e see enormous potential in AI – truly immense potential. At the same time, the possibility of misuse and wrongful application is, of course, a major problem. Technology always needs to be placed within a certain framework to keep such misuse at least somewhat under control. That's why there is broad consensus on the issue of prohibited systems, such as those related to surveillance or profiling." (Jungheinrich AG)*

In the context of the current deregulatory turn, civil society organizations – many of which were initially critical of the AI Act – now largely welcome and even defend it. As calls for deregulation grow louder, these groups increasingly see themselves as guardians of the existing regulatory framework. At the same time, they continue to point to the Act's shortcomings, including the withdrawal of the AI Liability Directive.

> *"It serves as a global model, one that other jurisdictions are also looking to. And it introduces concrete measures, concrete regulatory approaches that are being tested through it. This is certainly to be welcomed, even though we maintain certain criticisms and continue to see further gaps." (CSO)*

Interviewees also express critical or ambivalent views, with a few articulating more fundamental objections.

> *"If it were globally binding for every country, every organization [...] the AI Act would be a good regulation: it would slow AI down which would be helpful for society to adapt to the changes. If we regulate only here, this leads to a major disaster for Europe's economy as a whole – not just for the AI industry." (Casten Kraus)*

The critique often centers on potential risks to European competitiveness and innovation (see the section on Implications below). Many concerns relate to the legislative process behind the AI Act. Several interviewees point to inconsistencies and political compromises that, in their view, illustrate the difficulty of balancing competing objectives.

> *"I think the problem is that this became a product of trying to do everything for everyone. So you're probably [trying to do] good for innovation. You're trying to be good for human rights. You're trying to get it for growing companies or large companies, and you ended up being suboptimal for everyone." (European AI company)*

Other interviewees emphasize that the Commission's approach was overly ambitious and insufficiently aligned with business realities. Company representatives, in particular, say that procedural ambition has come at the expense of practical clarity. They note that the AI Act focuses primarily on protecting users rather than enabling innovation or supporting companies, leaving the perspectives and needs of those developing and deploying AI systems under-represented. Some also describe what they see as a "catch-all" tendency in European rulemaking – a preference for completeness that can undermine practical implementability.

> *"It also depends on the way the legislation is drafted. Sometimes you have a piece of work that is clear, and it's wonderful because you don't need much work to interpret it afterwards. But when you have this ambitious legislation that aims at grasping everything, like commercial and consumer technology plus sectors, and try to adopt provisions to regulate it all at once, the numbers of subsequent questions that are left unanswered is sometimes staggering. And also, unfortunately, it often reveals the way that the Commission ignores how business is actually done, how exchanges and discussions actually happen between companies and customers." (SAP)*

While civil society organizations welcome the AI Act as a rare instance in which law and technology have progressed in parallel, they also note that the final legislation reflects a series of compromises.

> *"It is probably the first time that technological and legal developments are progressing more or less in parallel. [...] Now, with the market readiness of ChatGPT and virtual reality, we have a legal framework emerging at the same time. [...] As a lawyer and legal scholar, I also recognize many technical shortcomings, which can, of course, be explained by the political process and the negotiations that I have also witnessed. [...] Much of it was drafted under time pressure, and many of the outcomes were simply compromises – typical of a broader societal negotiation process." (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie)*

Taken together, these perspectives suggest that criticism of the AI Act does not reflect opposition to regulation itself, but rather a concern – voiced most strongly by companies – that certain provisions are implemented in ways that make them difficult to apply in practice.

Despite this criticism, companies report they are actively preparing for the Act by building internal capacities, governance structures and workflows to operationalize compliance. They are working to embed AI governance within their existing operations as part of routine compliance, including integrating required measures directly into day-to-day development processes.

> *"At the end of the day, we are certainly aware that this could affect us – especially since we operate in the HR field. That´s why, for us as a company, the current approaches come as no surprise. We began preparing for them at an early stage – conducting risk analyses, thoroughly validating our systems, and embedding safety, testing and transparency mechanisms into our architecture. These requirements are by no means unfeasible. In fact, transparency measures such as documentation obligations have always been part of what we at Empion consider excellent engineering practice. So, when the regulation comes, we'll be prepared." (Maria Zerhusen, Head of Research, Empion GmbH)*

Moreover, larger companies in particular report that they have begun formalizing comprehensive compliance systems, embedding regulatory processes across departments and ensuring managerial oversight.

At the same time, the implementation phase introduces significant regulatory ambiguities and practical challenges, creating an atmosphere of uncertainty and, in some cases, fear across sectors. This uncertainty stems from the challenges organizations face in translating the AI Act into practice amid procedural opacity and institutional delays.

> *"We still don't know what the outcome will be. We also don't know how we will eventually be audited – there isn't even a designated body yet for the AI Act. ... So right now, there's a great deal of uncertainty for us. From a manufacturer's perspective, the question is: what do we actually need to do already, and what should we postpone – focusing, from an economic standpoint, more on innovation rather than on building additional processes and integrating them into development?" (Doreen Soeder, Head of Compliance, Tiplu GmbH)*

This uncertainty leaves organizations caught between preparation and hesitation, unsure whether to invest in compliance structures or wait for clearer institutional guidance. These perceived uncertainties are amplified by tight timelines, with several interviewees describing the implementation deadlines as "impractical" or "simply not feasible" (Dr.-Ing. Julia Hoxha, CEO, Zana Technologies GmbH). Companies worry that regulatory guidance released only shortly before key provisions take effect provides too little time to adapt.

From the perspective of some civil society organizations, however, such delays and last-minute adjustments are not due solely to bureaucratic inefficiency. They also view them as a byproduct of lobbying dynamics within the legislative process itself.

> *"Of course, I completely understand that we also have to take economic interests in this area into account. But many of the problems, such as the delays, are actually closely linked to the economic actors themselves. So I find it somewhat problematic, even hypocritical, to cause delays and then turn around and say: "Now that there are delays, we need to reopen the entire discussion." (Jürgen Bering, Gesellschaft für Freiheitsrechte)*

From the perspective of companies, by contrast, the implementation process is demanding on a practical level. Many point to operational and resource constraints that complicate compliance efforts. They describe the increasing complexity of aligning development processes with evolving legal requirements, as well as the disproportionate administrative and staffing burdens this alignment entails.

> *"[T]hese are of course aspects we now have to take into account during development. We need to factor them in and build in new loops. Especially as an AI developer [...]. That means every time we now have to run an additional loop through compliance and legal review, which simply takes time." (SME, legal tech)*

Finally, respondents identify the absence of institutional support structures as a central obstacle to implementation. The lack of clearly defined authorities or points of contact at both the EU and national levels is widely viewed as a major barrier, leaving organizations uncertain about where to turn for guidance. Several interviewees noted that this institutional gap

not only slows compliance efforts but also undermines confidence in the broader governance framework.

> *"The EU still needs to improve coordination at the interface level – including among its supervisory bodies. While the AI Office declares responsibility and urges compliance, the AI Act assigns key roles to national authorities – market surveillance, reporting obligations and oversight. Yet in Germany and many other Member States, these structures remain neither legally defined nor institutionally established. While the EU AI Office is ready to become operational, many Member States still lack this supervisory authority. Some even plan multiple separate offices, making the overall framework fragmented and difficult to enforce in practice. So it's really not very well coordinated." (Maria Zerhusen, Head of Research, Empion GmbH)*

These observations reinforce the perception that the Act's institutional architecture remains fragmented and underdeveloped. The resulting uncertainty leaves companies unsure how to operationalize compliance obligations, particularly in relation to reporting and auditing duties.

Taken together, these accounts point to a broader pattern of institutional lag, in which regulatory ambitions are seen as outpacing administrative capacity. Companies, in particular, frame their concerns around insufficient coordination and limited dialogue, calling for more structured interaction between policymakers and implementers to make the Act's objectives practically achievable. While the AI Act is widely regarded as a significant step toward trustworthy AI governance, its implementation is seen as introducing not only administrative burdens and resource constraints but also uncertainty and friction – conditions that set the stage for a more substantive critique.

## 2. Substantive critique

Beyond implementation challenges, stakeholders voice broader substantive concerns about the EU AI Act. One central thread of critique involves insufficient harmonization across the EU's digital regulatory landscape. Interviewees describe how overlapping regimes create simultaneous – and at times conflicting – obligations for the same technologies and business areas. They attribute this fragmentation to limited interinstitutional coordination, with legislative initiatives developed in parallel across different directorates and without adequate alignment. The result, they argue, is a patchwork of contradictory or redundant requirements.

> *"We have often seen that there are overlaps between EU legislations. This is partially due to the fact that they are prepared by separate Commission units, each pursuing its own specific objectives. Insufficient coordination and communication among these units can result in inconsistencies, redundancies, or even contradictions between legislative proposals" (SAP)*

In addition to overlapping regimes, respondents point to duplication in documentation and reporting obligations. They note that existing regimes already require much of what the AI Act mandates, increasing the administrative burden without delivering proportional benefits.

> *"EU policymakers are focusing a lot on incident reporting because we have reporting [duties] in the AI Act, the Data Act and cybersecurity legislation. At many instances we probably will be talking about the same incident." (SAP)*

> *"[There are] many duplications – double documentation obligations with different approaches but similar content." (Industrial engineering company)*

A further source of friction lies in definitional inconsistencies across legal instruments, which can lead to divergent classifications and obligations for the same

data or systems, a dynamic that undermines regulatory clarity.

> *"There are a lot of overlaps and even conflicts where one law says one thing and another law says another thing, because you have unclear definitions." (European AI company)*

For instance, one company describes how differing definitions of "biometric data" (BMW Group) in the AI Act and GDPR may lead to inconsistent classifications and additional compliance obligations. Similarly, a "compliance dilemma" (European DIGITAL SME Alliance) has been observed with regard to fairness testing, where requirements under the AI Act and the GDPR appear to conflict.

> *"The restriction on using sensitive data, even for fairness testing, raises practical concerns. Ensuring nondiscrimination often requires testing against sensitive attributes to detect bias. For SMEs, the lack of clarity on how to balance data protection under GDPR (Art. 9) with fairness testing obligations under the AI Act (Art. 10(5)) creates a compliance dilemma. Without explicit guidance or legal pathways (e.g., anonymization methods, safeguards for fairness testing), SMEs may be unable to prove compliance with bias requirements, despite having the intent to do so." (European DIGITAL SME Alliance)*

CSOs also also point to a clear "delta" (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie) across different EU digital regulations, which they attribute to the nature of democratic lawmaking – involving multiple actors, separated powers and asynchronous timelines rather than a coordinated, technocratic process.

Beyond insufficient harmonization within EU digital regulation, companies also point to overlaps and tensions between horizontal and sector-specific (vertical) regulations.

> *"The AI Act was designed to be the overarching regulatory framework, yet we lack real harmonization with sector-specific regulation. Instead of one clear compliance path, we now face two parallel, overwhelming regimes. And it's unclear if or when they will truly converge. The promise is alignment, but right now it's more a prospect than a guarantee. Implementation will decide if this becomes clarity or just layered complexity." (Dr.-Ing. Julia Hoxha, CEO Zana Technologies GmbH)*

Similar to the lack of harmonization in EU data regulation, interviewees observe that overlapping obligations create unnecessary duplication and administrative complexity.

> *"[W]here we see a big overlap definitely is for the conformity assessment required under the AI act and the MaRisk requirements under AT 4.3.5. There we have like more or less 90% overlap. [...] There are many requirements [such as concerning] risk management system [that is] more or less one on one what is required under article 9 of the AI Act, so for a bank that's duplicating documentation. Same for quality management system, Article 17 of the AI Act [which] we already have under 83 of the MaRisk and 84.4 compliance and risk controls." (N26)*

> *"We already have a lot of duplication, because much of what the MDR already implicitly requires is now made explicit through the AI Act – for example, data quality or risk management regarding bias and similar topics... Ideally, we would continue to have one conformity assessment procedure with our notified body, and they would simply extend their checklist with the AI Act requirements ... and that would be it. If we had to start separate conformity assessments or involve other auditors, that would be extremely burdensome – especially for smaller companies. We could probably still manage it, but such audits are always a huge effort." (Doreen Soeder, Head of Compliance, Tiplu)*

> *"In mechanical engineering, so much is already regulated, and we already have to comply with numerous ISO standards [...] yet there is no align-*

*ment at all. [...] Wherever we are already obliged to do something, we shouldn't have to do it twice. That should be the goal." (Industrial engineering company)*

Particularly in highly regulated industries such as healthcare and finance, where comprehensive risk management standards already exist, the only "really new" element is seen to be "human oversight" (Doreen Soeder, Head of Compliance, Tiplu GmbH).

*"As a fully regulated financial institution, we already have many of these elements in place. We do risk assessments, we do business management, and many more things that are already required by the MaRisk. While we are working on the whole framework to meet the AI Act requirements, a lot of the requirements are already in place due to the fact that we are regulated." (N26)*

They further stress that the lack of coordination between the AI Act and sectoral frameworks such as the Medical Device Regulation (MDR) not only increases the burden on firms but also strains the capacity of supervisory authorities.

*"[I]f you get your MDR approved by one notified body, and let's say that notified body is booked and can't do your AI review until later then, but there's still potential information they require from the MDR and vice versa, right? So, like the importance of having these combined. Because you are duplicating effort not only for yourself but also for the notified body if they have to review the same device twice, it's a lot more efficient to combine for the notified bodies who are slammed and they're overworked and they're not enough of them to kind of handle the demand. And also, for the companies, right. That want to get it done quickly, efficiently." (Dr.-Ing. Julia Hoxha, CEO Zana Technologies GmbH)*

Rather than aligning with established sectoral regulations, the AI Act is described as introducing parallel procedures that heighten compliance burdens and dilute regulatory coherence.

*"The transition from MDD to MDR has pushed most AI/digital health technologies into higher-risk classifications, demanding notified body review. With the AI Act now entering force, manufacturers face overlapping and potentially conflicting compliance pathways. Without clear guidance on mutual harmonization – ensuring MDR compliance also satisfies AI Act requirements – we risk creating redundant assessments that slow down innovation." (Dr.-Ing. Julia Hoxha, CEO Zana Technologies GmbH)*

Conflicting requirements between sector-specific regulation and the AI Act are also noted – for example, regarding the sequencing of clinical evidence. Under the MDR, clinical evidence must be generated before a product receives CE marking (Conformité Européenne), whereas the AI Act appears to imply that CE marking should precede clinical evaluation.

Interviewees further emphasize definitional inconsistencies, noting that key terms are defined differently across the AI Act and existing legislation, adding another layer of ambiguity for compliance. As a result, uncertainty extends beyond overlapping obligations to encompass the interpretation and operationalization of regulatory concepts, particularly where horizontal and sector-specific regimes intersect.

*"The definitions of 'safety components' don't align between the AI Act and the respective harmonization legislation. ...The AI Act's definition is relatively broad and may capture more components than type approval would, requiring further interpretation." (BMW Group)*

Respondents also express concern that layering the AI Act onto existing sector-specific regimes may not necessarily enhance safety or accountability. The automotive sector illustrates these tensions particularly clearly. The coexistence of the AI Act with established vehicle type-approval procedures not only adds administrative burden but also heightens uncertainty. Companies note that unresolved questions – such as whether, when and under which implementation

timelines the AI Act's requirements will be integrated into type approval – create substantial ambiguity. They also struggle to understand how the Act's obligations will fit within the long-standing type-approval framework, especially since products covered by that framework already meet extensive safety requirements.

> *"The open question is: does [a break assistant] become safer if we now additionally regulate it under the AI Act, or do we create uncertainty? [...] And beyond the question of when it comes, there's also the question of how – will the AI Act simply be copied and pasted into type approval, leaving us with the same problems, or will it be carefully adapted to the vehicle context?" (BMW Group)*

Another thread of substantive critique concerns the AI Act's risk-based approach. Overall, interviewees broadly acknowledge the logic of a risk-based approach.

> *"[W]e are in favor of a risk-based approach. So, we like it, and not only in AI regulation but in all security regulations." (SAP)*

Companies view the risk-based approach as a pragmatic and familiar regulatory principle that can meaningfully differentiate among levels of potential harm. In that sense, the framework is regarded as both reasonable and consistent with existing product-regulation logics.

> *"It makes sense that when AI is used in a certain area, higher requirements apply there – generally speaking – than in other areas." (SME, legal tech)*

While some emphasize its conceptual clarity, others highlight practical advantages, noting that the framework allows companies to calibrate compliance according to the specific risk categories. For many, this adaptability makes the model workable and proportionate in daily practice.

Despite these generally positive assessments, companies also describe the Act's broad definition of "high-risk" systems – and the associated obligations – as "neither understandable nor feasible to implement" (Jarek Kutylowski, DeepL). Several argue that portraying high-risk systems as inherently dangerous leads to "extreme obligations imposed on developers," which they see as an instance of "legislators shifting responsibility onto developers" (Jarek Kutylowski, DeepL).

The classification framework is viewed as introducing uncertainty rather than clarity, given that distinctions between risk categories often remain ambiguous in practical contexts. According to companies, this lack of precision complicates planning and resource allocation throughout the development cycle.

> *"I have lots of questions. Are we prohibited, high risk or are we low risk? [...] The basic issue of the risk category has multiple considerations, and [the risk category] impacts all your product development in terms of resources, time, energy and also the sales cycle." (Dr. Sejal Tolksdorf, Regulatory Pathfinder)*

In the perceived absence of concrete examples or case-based guidance, companies find it difficult to determine where their systems fall along the risk spectrum.

> *"When does one move from [limited] risk to high risk? These are exactly the kinds of clarifications that were supposed to be illustrated with examples at the EU level – but which still haven't materialized." (Industrial engineering company)*

Moreover, interviewees question whether risks can meaningfully be predetermined through fixed categories. They argue that the potential impact of an AI system depends heavily on its specific context of use – a factor that cannot be reliably assessed during development.

> *"The AI Act implements specific regulatory measures without the ability to fully anticipate their actual outcomes – particularly regarding the risk classification of individual AI systems or their out-*

*puts. Such assessments are inherently difficult to determine ex ante, as they are highly dependent on the specific application context. These preliminary evaluations often remain so indeterminate that, despite its well-intentioned aims, the AI Act may constitute one of the most significant impediments to innovation within European regulatory frameworks." (Maria Zerhusen, Head of Research, Empion GmbH)*

CSOs warn that unclear definitions and filtering mechanisms within the Act may create loopholes or enable strategic misclassification. The lack of clear boundaries between risk levels – especially in sensitive domains such as justice – is seen as opening the door to inconsistent interpretations or even misuse.

*"So where is the boundary? When is it considered a substantial contribution, given that the judiciary, for example, is also an area that in certain cases is viewed as high-risk. And that is exactly the point. We said: 'That sounds to us like a loophole to opt out.' And it is simply not clearly defined to the end. That is why we criticized it." (CSO)*

In addition, company representatives widely emphasize that the AI Act leaves critical questions of accountability along the AI value chain unresolved. They describe a legal uncertainty" (Jarek Kutylowski, DeepL) regarding how responsibilities are divided between providers and deployers, particularly when general-purpose or fine-tuned models are involved.

*"The provider is not able to give the deployer all the information, because they don't know what I will use it for. That is, of course, a chicken-and-egg problem." (Jungheinrich AG)*

This dilemma is discussed most prominently in relation to the fine-tuning of GPAI models. Although guidelines exist, interviewees note that critical obligations – such as ensuring copyright compliance or disclosing cybersecurity resilience – can only be fulfilled by the original model provider. Yet once fine-tuning passes a certain threshold, accountability becomes blurred.

*"What, in my opinion, remains unresolved is that once you cross that threshold of fine-tuning, there are obligations that only the model provider can fulfill, for example, when it comes to a copyright compliance strategy or disclosing cybersecurity resilience. But then who takes on these obligations?" (BMW Group)*

For companies, this creates a practical concern: if fine-tuners are expected to assume these obligations, they must rely on assumptions that depend on the degree of transparency or architectural disclosure by the model provider. At the same time, requiring original providers to remain responsible for cybersecurity risks in substantially modified models raises its own set of challenges.

Moreover, the transitional provisions for fine-tuning under Article 111 are also widely viewed as unclear. Interviewees note uncertainty about whether adaptations exceeding the FLOP threshold would be treated as creating a "new" model – which could invalidate transitional periods and trigger full compliance obligations when entering new markets.

*"There's Article 111(3) on transitional periods when a model has already been placed on the market. [...] If we fine-tune the model for each jurisdiction, at what point does it become a new model? From when can we rely on the transitional periods for the old one? [...] For Germany, that seems clear, but for other markets launching later this year, it remains uncertain." (SME, legal tech)*

This critique highlights a deeper structural tension in the Act's design: by targeting AI as a cross-sectoral technology, the Act challenges traditional product-based accountability models and creates gray zones over who ultimately bears responsibility for compliance and potential harms.

*"It creates this dynamic of what are you responsible for and what are you not? [...] This comes from the unclear definitions, and [...] the basic problem of trying to regulate technology rather than products, because if you just talked about products,*

*then it would always be the company selling the products responsible, and it's sort of clear cut who is responsible for what?" (European AI company)*

Across interviews with company representatives, a recurring concern is that the AI Act's approach – while intended to ensure comprehensive oversight – risks both diffusing accountability and constraining technological development at its source.

*"The primary concern lies in the fact that the AI Act does not merely regulate end users, but also the underlying technology itself. You can think of it like this: one would not seek to regulate a computer simply because it could be misused to compose a ransom note. Yet under the AI Act, this foundational technology is subject to regulation, a measure that inherently constrains innovation and impedes further technological advancement by restricting it at its very core." (Maria Zerhusen, Head of Research, Empion GmbH)*

Interviewees also point to challenges associated with using open-source models in high-risk applications that result in a paradox. While open-source models are widely regarded as critical drivers of innovation, their deployment creates significant compliance difficulties because companies often lack transparency into, and control over, the underlying data and training processes.

*"With open-source models, we have no real insight into how they were trained, which makes it extremely difficult to ensure compliance in high-risk contexts." (SME, legal tech)*

Finally, interviewees consistently identify documentation obligations as one of the most burdensome aspects of the AI Act.

*"What this results in is a duplication of documentation that places an additional strain on our teams. For highly regulated institutions like ourselves, we would wish to see the additional requirements included as an amendment to the existing MaRisk framework, such as adding the requirements related to human oversight, rather than entirely separate sets of legal requirements with a high degree of overlap, resulting in significant duplication of work. We believe we could do that under AT 4.3.5 already." (N26)*

They view the requirements as excessive and, in some cases, redundant, particularly for organizations operating across multiple jurisdictions or subsidiaries. Meeting transparency and record-keeping expectations is described as demanding substantial administrative effort and coordination.

*"The transparency aspect is good, but I would prefer to simply register it rather than having to produce and maintain those 20 or 50 required documents – which is the far worse part. I'm not just creating them; I also have to keep them up to date. That's something where our data storage is filling up more and more, and I honestly don't yet know how to handle this monster, especially when changes occur." (Jungheinrich AG)*

These obligations translate into significant compliance costs, particularly for SMEs and startups that must allocate resources for compliance from the outset of product development.

*"Well, one point for us, of course, is that financially this will be a huge burden coming our way. I mean, the high-risk provisions only take effect next August, but of course, it's something we already have to consider now. We need to obtain expert opinions, and our customers are already asking: do you have this on your radar? What can you already do? It's clear that we'll have to change our internal processes." (SME, legal tech)*

These accounts illustrate how compliance obligations extend far beyond the Act's formal entry into force, generating substantial anticipatory administrative effort and financial strain – burdens that fall disproportionately on actors with limited internal regulatory capacity. As one interviewee notes, a startup "has to hire both the CTO and the regulatory officer from day one, especially when you go into the space

of being what they call a high-risk device." This dual focus on innovation and compliance "is a challenge and a burden in terms of expense" (Dr.-Ing. Julia Hoxha, CEO Zana Technologies GmbH), especially for small companies with constrained budgets.

CSOs, by contrast, criticize the documentation requirements for lacking transparency, noting that very little of the information is made public – as illustrated by minimal disclosures in the Article 70 database – which in turn limits external oversight.

> *"There are, of course, many transparency mechanisms in principle, but there's also a lot of skepticism, both on our side and within civil society more broadly, about whether these instruments will be helpful in practice, as the information that is available to the public and CSOs is limited and individual rights leading to transparency are arguably limited in comparison with, e.g., the GDPR." (Jürgen Bering, Gesellschaft für Freiheitsrechte)*

In sum, these accounts reveal a substantive critique that extends well beyond implementation hurdles. Companies, in particular, describe a fragmented regulatory landscape characterized by overlapping and sometimes conflicting obligations, duplicative documentation and assessment requirements, and definitional inconsistencies that undermine legal certainty. Although the risk-based approach is broadly acknowledged, its boundaries and practical operation remain unclear, especially for modular systems, GPAI models and sector-specific use cases. Accountability along the value chain is seen as insufficiently defined, particularly after fine-tuning, producing gray zones between providers and deployers. Documentation obligations are widely viewed as excessive, opaque and costly, with disproportionate effects on SMEs and startups, while offering limited public transparency to support external oversight. These concerns shape expectations about the Act's implications for innovation, market dynamics and Europe's technological competitiveness, which the next section examines.

## 3. Implications

Several interviewees express concern that the AI Act may inadvertently slow down AI development and adoption across Europe. To manage regulatory uncertainty and reduce administrative burdens, some companies intentionally limit or avoid the use of high-risk AI systems, even when doing so constrains business opportunities. They also report increasing reluctance among clients, who – confronted with the AI Act and other EU data regulations – hesitate to adopt AI for fear of legal consequences and associated costs. As a result, companies must devote additional effort to reassuring customers and guiding them through compliance procedures.

> *"There's definitely a strong sense of hesitation. Many users are hesitant to deploy AI systems, fearing potential non-compliance in the future. This reluctance stifles adoption, monetization, and ultimately investment in European foundational research. While the reference to prospective sanctions may be legally sound, it does little to alleviate the palpable uncertainty experienced in the present – not that deals aren't being closed because of it; I would say that by now we are sufficiently prepared and fully understand these concerns, enabling us to address them effectively." (Maria Zerhusen, Head of Research, Empion GmbH)*

Others observe that this uncertainty directly affects market access and customer relationships. While large corporations can rely on dedicated compliance departments to manage regulatory complexity, smaller clients may refrain from deploying AI altogether.

> *„And then it will probably have an impact later in much more complicated market access, because we'll likely see growing skepticism among customers and users. When, say, Daimler comes along, it's not such a big issue – they have departments and people who handle compliance checks. But if I have a smaller licensee who wants to, for example, monitor the safety of their machines and see*

*whether someone has a facial expression in front of the machine so it can stop automatically – well, if I want to do something like that, the question becomes: am I even allowed to do this in the EU? And then they get uncertain. I've seen this at many client meetings where, when I just ask straightforwardly, people are completely unsure: what am I actually allowed to do, and what not?" (Carsten Kraus)*

In addition to hesitancy in AI adoption, companies report longer product development cycles. Frequent compliance checks, documentation duties, and potential reclassifications extend project timelines and delay innovation.

*"[T]here was some concern from management that this could cause further delays in bringing our medical products to market. Right now, we still have a medical device in development and that, since the effort required for MDR compliance is already enormous, any additional tightening of regulations would make things even harder." (Doreen Soeder, Head of Compliance, Tiplu GmbH)*

The perceived regulatory complexity also encourages greater caution in using AI tools internally, as organizations hesitate to integrate technologies whose risk profiles or compliance implications remain unclear.

Finally, respondents link these patterns to rising investor skepticism. They argue that heightened compliance costs and legal uncertainty undermine the attractiveness of AI ventures, particularly for early-stage startups.

In response to the regulatory uncertainty surrounding the AI Act, interviewees observe a range of strategic adaptations emerging across the market. Some organizations and their clients are are beginning to reference compliance in procurement processes, indicating that the Act is already shaping contractual expectations even before it fully takes effect. Yet these references are often vague and lack clear criteria, reflecting the absence of standardized guidance or broadly understood benchmarks for what AI Act compliance entails. Firms report that tenders and client requests increasingly include compliance-related clauses, but these clauses are typically so broad that they are difficult to operationalize.

*"[Y]ou can sense a certain uncertainty. For example, we have a tool for writing medical letters, and that's not a medical device – it's really just meant to support documentation. But it's based on an LLM, and you can already see vague wording in tenders, like: 'The product currently and in the future meets all legal requirements that may apply.' And we're supposed to handle that. And the second issue we're increasingly noticing is that we're getting inquiries from customers – compliance officers, data protection officers, and so on – asking: 'How are you handling this?' So, some are already being proactive. But I think there's still not much expertise in the market yet, especially on the client side, when it comes to procurement. So, there's nothing particularly concrete there yet." (Doreen Soeder, Head of Compliance, Tiplu GmbH)*

Interviewees also describe a growing tendency among companies to adopt pragmatic – and at times calculated – strategies for navigating regulatory ambiguity. In the absence of clear enforcement mechanisms, compliance has become partly a matter of strategic timing rather than strict obligation, with some firms deliberately postponing full implementation of the AI Act's requirements until supervisory structures are fully in place.

*"To be honest, those who genuinely want to comply – who take the regulation seriously – are at a clear disadvantage right now. They have to invest significant resources to understand and implement nearly a thousand pages of legal text, while others simply ignore it because there are no enforcement authorities yet. Without clear guidelines and functioning control mechanisms, the ones who play by the rules are the ones who lose out." (Maria Zerhusen, Head of Research, Empion GmbH)*

Others note that this uncertainty has turned compliance into a balancing act between prudence and

pragmatism. Firms must decide whether to act preemptively or wait for regulatory clarification, weighing the risks of non-compliance against the costs of overcompliance.

> *"And the question will be: how much willingness to compromise will find its way into these regulations? How much room for interpretation will there be? We're working very much with these implementation waves – asking ourselves, what do we have to do now? Should we already go beyond compliance? Or should we wait and see? Or should we strike a reasonable compromise by saying that the penalties can't be too severe if we've fulfilled certain basic requirements and have compliance more or less under control? And to me, that's the wrong approach." (Industrial engineering company)*

Some interviewees describe how organizations are already developing strategic narratives to navigate regulatory ambiguity. In the absence of clear definitions and enforcement mechanisms, firms adjust their internal and external communication to position their products in ways that minimize perceived regulatory exposure. This often involves emphasizing distinctions not explicitly recognized in the AI Act to reassure clients and maintain marketability, while postponing definitive technical classification until greater regulatory clarity emerges.

Taken together, these practices illustrate a form of regulatory navigation in which compliance becomes negotiated, selective and responsive to uncertainty rather than a straightforward legal process. Yet the ability to engage in such navigation depends heavily on organizational capacity. Respondents underscore that this uneven distribution of regulatory burdens creates a structural imbalance: SMEs face disproportionate challenges in meeting compliance requirements compared with larger corporations that have dedicated legal teams and more substantial financial resources.

> *"The large companies ... have big legal departments and the resources to hire external law firms. [T]he smaller the organization, the fewer resources there are to deal with such issues. And if we look at how quickly you can run into trouble and how many things you have to consider when using AI – including what's still unclear – I think the smaller the organization, the harder it is to remain compliant. Or it might even lead companies to avoid using AI altogether for that very reason." (SME, legal tech)*

For smaller firms, the administrative effort required to ensure compliance creates tremendous difficulties. The volume and complexity of the regulation demand substantial time and expertise that few can afford.

> *"For smaller companies, compliance is virtually impossible due to limited resources. If you look at the AI Act, it's about a thousand pages long. What medium-sized company, or especially which startup, has the capacity and resources to really go through it properly? Achieving full compliance could take a long process, and by the time one finishes, new developments have already emerged." (Maria Zerhusen, Head of Research, Empion GmbH)*

Even firms that began preparing proactively for the AI Act report feeling constrained by limited internal capacity. Early compliance work often depends on technically skilled employees who assume regulatory responsibilities in addition to their primary roles.

> *"We started early and began allocating resources to this as soon as possible. I'd say for about a year and a half now, I've been working with an ML developer who's also interested in regulatory topics to assess the relevance of the AI Act for us and translate it into corresponding processes. Personally, I believe in strong system competence – it's more important than individual expertise. But of course, there are certain concerns that come with this, because as a relatively young, newly medium-sized company, our resources are not unlimited." (Doreen Soeder, Head of Compliance, Tiplu GmbH)*

Regulatory asymmetries between large and small companies also play out in the marketplace, where perceived compliance becomes a competitive advantage. Clients increasingly gravitate toward large, established providers, assuming their solutions are more compliant and therefore pose less risk.

> *"The big providers like Adobe or Microsoft already offer a solid basis and take their obligations seriously, but among mid-sized and smaller tool vendors we still see major deficits." (Jungheinrich AG)*

At the same time, regulatory complexity and uncertainty are seen as deterrents to new entrants. Several respondents voiced broader concerns that Europe's well-intentioned regulatory environment may inadvertently discourage entrepreneurial experimentation and stifle innovation.

> *"The EU AI Act adds [...] another layer of complexity [and] [...] scares [...] startups" (Dr.-Ing. Julia Hoxha, CEO Zana Technologies GmbH)*

These accounts suggest that the AI Act may inadvertently reinforce existing market hierarchies. While large firms can leverage compliance as a signal of reliability and trust, smaller firms face rising barriers to entry. The resulting disparities risk consolidating market power among established players and discouraging innovation and experimentation among startups and SMEs – the very segment expected to drive much of Europe's AI development.

Companies anticipate that these combined implications will ultimately hamper innovation in Europe, warning that "[t]hat we ultimately end up deterring innovation and effectively stifling this drive to innovate" (Doreen Soeder, Head of Compliance, Tiplu GmbH). Companies thus raise concerns regarding the AI Act's potential impact on Europe's global competitiveness. Several note that the Act's compliance requirements risk concentrating market power among large companies – especially U.S.-based technology firms – because these firms can more easily absorb regulatory costs. As a result, SMEs in the European market may face a structural disadvantage.

Companies note that EU legislation tends to favor large, established firms that can absorb compliance costs, whereas smaller or growing businesses struggle to scale and compete effectively. This, they suggest, helps explain the relative lack of major European players. This uneven distribution of regulatory burden not only reinforces existing hierarchies but also diverts resources from innovation toward administrative obligations.

> *"[W]e're already seeing a significant competitive disadvantage, because we have to invest more and more personnel and consulting resources into complying with this Act – resources that actually add no real value." (Industrial engineering company)*

Beyond compliance costs, respondents emphasize that the Act may unintentionally weaken Europe's innovation momentum. Companies fear that excessive caution and regulatory complexity are fostering a culture of risk aversion that constrains experimentation.

> *"We all want AI systems where the human makes decisions, but within a few years, we're going to have authentic AI systems that are going to be better decision makers than humans on things that are not that important. [...] So American companies are going to be able to do performance management completely automated within two years. And in Europe we're still going to have to have huge HR departments of people filling out form, telling you, you did five or you did four last quarter, which is ridiculous because it's still a subjective measurement. So, it's not that it's any fairer in Europe. It's just because we decided that we're a little scared of the machines, and we want to have human in the loop. And because it sounds good. And so that's an issue I see in the future." (European AI company)*

As a result, many interviewees worry that the AI Act could undermine Europe's global competitiveness. They warn of a potential erosion of technological sovereignty, as compliance demands draw resources

away from innovation and inadvertently deepen Europe's dependence on external technologies and models.

> *"Others are moving ahead at tremendous speed, while we'll end up becoming dependent on their AI systems. Here is the thing: Generative AI systems, particularly LLMs, are mindset machines. As a result, through the mindsets embedded in their language models, our European culture will end up being dominated by them. And 'culture' here includes all our economic and social ways of thinking." (Carsten Kraus)*

Finally, divergent regulatory frameworks across jurisdictions are seen to further complicate international deployment. Companies operating globally face mounting compliance fragmentation that slows product rollouts and multiplies administrative work.

As a counterpoint, civil society representatives challenge the narrative that AI regulation poses a threat to Europe's competitiveness. Rather than viewing the AI Act as an obstacle, they see it as a necessary step toward embedding democratic values and accountability in technological development. From this perspective, Europe's slower pace reflects deliberation and robust democratic processes that prioritize oversight and rights protection over unrestrained technological acceleration.

> *„We don't even know yet how the provisions of the AI Act will work in practice, but people already suggest that the EU will stifle innovation [...] [But] what kind of innovation, and for whom? Does it serve the common good or just those who control those technologies? The AI Act was drafted in a lengthy and intense legislative process. It should now be respected and enforced – instead of trying to open the whole package once more in favor of certain stakeholders with huge lobbying power. Now, it will simply take time to find out where adjustments might be needed. I don't believe Europe will fall into misery if we start enforcing the AI Act now [...]." (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie)*

Taken together, the findings show that the AI Act is reshaping market behavior and organizational strategy, even before it is fully enforced. Compliance has become a factor in competitive positioning, influencing investment decisions and procurement practices. Yet this early adaptation also exposes structural imbalances: large firms can absorb uncertainty and even leverage compliance as a competitive strength, while smaller actors face growing administrative barriers and reduced room for innovation. At the same time, civil society voices stress that the Act's significance extends beyond market competition, framing it as a democratic instrument for ensuring accountability, transparency and the protection of fundamental rights in technological development. The challenge, they argue, lies in ensuring that Europe's commitment to rights and accountability does not come at the expense of its capacity to innovate and compete globally.

## 4. Proposed actions

Beyond identifying challenges and unintended consequences of the EU AI Act, interviewees also offer a wide range of suggestions for improving its implementation and long-term viability. Across stakeholder groups, there is broad agreement that the Act's success will depend primarily on how it is operationalized in practice. Rather than reopening the legislation, stakeholders emphasize the need for refinement – pragmatic adjustments rather than structural overhaul. One of the most frequently mentioned proposals concerns the implementation timeline, which is widely viewed as overly ambitious given delays in finalizing technical standards and guidance documents.

> *"[We are faced with an] overly ambitious process and timeline. The easy solution is, looking at it with hindsight would have been just a longer implementation timeline. Basically, instead of 2025, August 2nd, it would have been 2027. They would have created three years for themselves to actually figure out what all this stuff means." (European AI company)*

More broadly, interviewees stress that the timeline does not reflect the planning cycles of businesses, which operate on much longer development and sales rhythms.

> *"I still think it would be good to reconsider the transition periods – especially with regard to the different timelines, including those for high-risk systems. I find next August to be quite ambitious, given how many things are still unclear, to be honest. The same goes for sales and development cycles; it somewhat misses the reality that companies need a certain degree of planning certainty." (SME, legal tech)*

This perceived mismatch between regulatory ambition and practical feasibility is particularly acute for SMEs, which rely on timely access to technical standards to avoid costly legal consultation.

> *"In that regard, it's clear that the big problem is that the technical standards under Article 40 won't be completed in time. As a result, SMEs in particular won't have the opportunity to access the central AI compliance tool of the AI Act to avoid incurring huge legal costs. That's one of the major issues, because these standards will very likely only be finalized around mid-month in August 2026 – yet by then, companies are already required to comply with the relevant provisions. Even if you managed to get it done within three months, by August, it wouldn't help." (SME, legal tech)*

Interviewees also emphasize that extending the timeline should be seen as an opportunity for mutual learning between regulators and industry, not simply as a postponement of compliance.

> *"It doesn't mean that I say to our teams: okay, it's delayed, you can stop, you can relax, you can take your coffee. [...] It means that we just have more time. And also, as I said, it's education to both sides. So, we explain to them what we do and how the technology can be adapted to what they want. And they explain to us what exactly they expect from the manufacturers." (SAP)*

Civil society organizations, by contrast, take a more critical view of broad calls for extending the timeline, warning that such measures could risk reopening the AI Act itself and undermine its implementation.

> *"I fear that postponing them would ease the pressure, leading us to have the same discussions a year later. From other areas, we know that public enforcement tends to be quite lenient at this stage, and in practice, there will also be a lack of personnel in the authorities to conduct proceedings. As a result, there will already be a de facto enforcement moratorium. A formal moratorium, however, would have the disadvantage that even deliberate and very serious violations could not be pursued." (Jürgen Bering, Gesellschaft für Freiheitsrechte)*

> *"I'm very skeptical about postponing the implementation period – that's exactly what Big Tech is working toward right now. [...] They deliberately delay the process, raising countless concerns at the last minute to push the timeline back and then argue that the application should also be postponed." (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie)*

If at all, a more targeted solution is proposed, such as a temporary moratorium for SMEs, whereby "in the first two years, small and medium-sized enterprises won't face strict enforcement ... to account for the specific circumstances of SMEs" (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie).

Interviewees also emphasize that beyond adjusting deadlines, the manner of enforcement will be decisive for the Act's success. They argue that compliance should not rely on immediate sanctions but should be accompanied by mechanisms that allow organizations to learn, adapt and build capacity over time. Regulatory sandboxes, some of which are already being piloted under the AI Act, are frequently cited as a practical means to bridge this gap. Such environments would enable companies to experiment with compliance procedures before penalties apply, fostering a culture of learning rather than fear.

> *"In order for innovators to thrive, enforcement shall only be pursued when solid compliance mechanisms, such as standards and sandboxes, are fully in place. Forcing enforcement prior to these conditions means dropping unnecessary burdens on SMEs." (European DIGITAL SME Alliance)*

The perceived absence of adequate supporting structures is regarded as a key obstacle. Without clear technical standards or supportive transition mechanisms, companies – especially SMEs – struggle to meet requirements while maintaining momentum for innovation.

> *"But as long as they don't exist yet – at least not for us in relation to the AI Act – there should either be clearer guidance on what exactly needs to be done, or the enforcement should be more lenient, or simply wait, so as not to create this gap. Otherwise, we'll just end up discouraging companies and effectively taking the drive for innovation out of them." (Doreen Soeder, Head of Compliance, Tiplu GmbH)*

Respondents stress that such sandboxes should not be left to industry alone but developed in close collaboration with regulators to ensure both legitimacy and accessibility. Publicly funded initiatives could lower participation barriers, particularly for smaller firms.

> *"This would work if done in collaboration with the regulators, not as a private initiative where one big player hosts a 'sandbox' and everyone else just shows up. We need true collaboration. Furthermore, SMEs and early-stage companies need to get financial support to test, apply guardrails, and learn in a real environment without having to build a full regulatory department before they have even figured out the product itself. Government-supported sandboxes could level the playing field and accelerate safe innovation, instead of slowing it down." (Dr.-Ing. Julia Hoxha, CEO Zana Technologies GmbH)*

This emphasis on support before sanction resonates across sectors. Rather than prioritizing penalties, several interviewees argue that the regulatory framework should provide corrective opportunities when companies act in good faith but lack full understanding.

> *"And that's why I think approaches that don't put sanctions front and center, but instead emphasize support in cases of misconduct, are so important. Why not say: [Company X] didn't act negligently – they did the best they could, but they simply had gaps in knowledge or implementation. So, let's give they the time to correct that. Why immediately throw around millions in fines? Risk and punishment shouldn't be the main focus, because then we lose opportunities. That's where we need to act – that should be the goal of this reform process." (Industrial engineering company)*

Company representatives consistently emphasize that the effective implementation of the AI Act depends on clear, coordinated and well-supported guidance structures. Across interviews, they express frustration with the lack of accessible, practical information that translates complex legal requirements into actionable steps for developers and operators.

> *"And clear guidelines are needed; when those guidelines exist, they should really be explained in a practical way. Not a 1,000-page legal text, but something short and concise. The Code of Practice is a good start, but it's another 100 pages. What's really needed is something that feels more like a 20-page brochure." (Maria Zerhusen, Head of Research, Empion GmbH)*

Companies argue that compliance would be far more attainable if the European Commission and national authorities provided predefined compliance templates and technical standards that could be directly used by AI developers. Such tools would not only reduce legal uncertainty but also ease the administrative effort currently required.

> *"Yes, what I find unfortunate is that companies are very quickly left on their own – also when it comes to registration. I would really like the EU to at least provide some kind of framework solu-*

*tion for registering use cases. Right now, everyone is just muddling through on their own.... I'd really like to see more support for companies, tools that actually help with regulatory compliance and offer guidance....There should be much more emphasis on this, because it would also help smaller companies engage more effectively with these issues." (Industrial engineering company)*

Civil society representatives echo this demand insofar as they recognize that the development of technical standards will be crucial for translating legal norms into operational practice. Standardization, they argue, is essential for bridging the gap between high-level legal principles and the concrete realities of development work.

*"There are legal requirements in the AI Act, which are then translated into harmonized technical standards. When an IT expert or programmer says, 'Here is a standard that needs to be implemented in our product' they will know what to do; but if you just tell them, 'Here is the law,' they don't. [...] That's why I consider standards an extremely important instrument [...]. I've worked in standardization myself and learned how to break things down to a level that can be implemented in products." (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie)*

Beyond technical standards, firms practical solutions such as a "one document" approach to counteract what they perceive as excessive documentation burdens.

*"This 'one document' approach is extremely important. We assume that in a year or two, almost every piece of software we use will include AI. That doesn't help us at all, because it means that if we don't counteract this with proper regulation, next year we'll spend all our time just documenting." (Industrial engineering company)*

Companies also urge authorities to focus on providing consistent, practical instructions, particularly for interpreting high-risk requirements.

*"We are awaiting [...] guidance on high-risk AI systems classification at the moment. Also, many things will depend on the national authorities that will be in charge of supervising and enforcing the law over the high-risk AI systems' providers in the capitals." (SAP)*

*"There are still some interpretation questions regarding the AI Act, where we are waiting for guidance from the EU AI office, as to enable us also to facilitate and simplify the classification of AI use cases." (N26)*

Participants further call for central points of contact and unified oversight bodies to avoid fragmented responsibilities across EU and national authorities, ensuring accessibility for companies and citizens alike.

*"You can't simply say, „We're implementing this now," when the supervisory authorities are still missing – that simply doesn't work. The Commission's AI Office may be ready, but at the national level – where market surveillance and oversight should take place – structures are still largely lacking. Without them, the practical implementation of the AI law and sanctions remains difficult." (Maria Zerhusen, Head of Research, Empion GmbH)*

Finally, SMEs stress that accessible guidance must be paired with targeted institutional support, including dedicated points of contact and funding opportunities to help smaller firms compensate for limited legal and compliance capacities. Such measures, they argue, would not only promote fairness but also ensure that regulatory compliance becomes an achievable goal rather than a competitive disadvantage.

From a civil society perspective, effective oversight requires not only coordination among authorities but also transparency and public accessibility through a central point of contact that allows citizens to navigate the system easily.

*"There's also the issue of enforcement and oversight structures. In Germany, there really needs to be careful consideration of how to implement this*

*consistently, because so many different authorities have already been designated, and on top of that, there's the federal division of responsibilities. It's crucial to ensure that this becomes a uniform and accessible system – something that an ordinary person, someone who just wants to find out some information, can actually navigate. That's what was originally intended, with a central point of contact, but it's really important to make sure this doesn't get fragmented through turf wars between the various authorities." (CSO)*

A recurring theme among company representatives is the need to simplify and better harmonize the regulatory landscape surrounding AI. Respondents emphasize that the AI Act should not stand in isolation but must be integrated into the broader ecosystem of EU digital and sectoral regulation. Interviewees call for clearer mapping across existing and forthcoming regulations, along with tools that make compliance more navigable across frameworks.

*"What we're really missing is something like a data regulation matrix... making these overlaps visible to avoid redundant work – is so important, because data regulation is incredibly complex. It's not just the AI Act and the Data Act; there are ten or fifteen other major regulations that affect your business model if you work with data or software – like the High Resilience Act, the Data Governance Act, the GDPR and other new directives. I could name dozens more that play a role. What's really needed – ideally supported by legislators – are administrative guidelines or a kind of data regulation matrix that shows, for instance: if you meet requirement X under the AI Act, you also meet requirement Y under the Data Act, and so on. It would be great if that didn't have to come from lawyers, because that's expensive – and something we can't easily afford." (SME, legal tech)*

Interviewees suggest that such alignment could be achieved through cross-regulatory recognition mechanisms, whereby compliance with one framework would automatically satisfy equivalent provisions in others.

*"Recognizing existing GDPR certification under the AI Act would greatly simplify compliance. If documentation already meets national requirements, there would be no need for duplication or re-evaluation – verification is already in place. This approach would respect documentation obligations while streamlining the process." (Maria Zerhusen, Head of Research, Empion GmbH)*

Several respondents point to the wealth of regulatory experience already available across European sectors, arguing that this accumulated knowledge should be actively incorporated into the AI Act's implementation.

*"When it comes to structural aspects, there's already more than enough experience – from the MDR, from the Machinery Directive, and now the Regulation. These are all things that could, in theory, be carried over, yet we're facing exactly the same questions again at the outset. [...] If the right people were brought together, I think there could be much better expertise in handling these matters, including in the finer details." (Doreen Soeder, Head of Compliance, Tiplu GmbH)*

At the operational level, companies also call for greater reliance on existing standards, allowing well-established frameworks to be adapted to meet the Act's requirements.

While civil society representatives recognize the value of alignment, they caution against equating harmonization with deregulation. Simplification, they argue, should enhance coherence without eroding protections. They warn that the current political debate risks using "regulatory simplification" as a rhetorical tool to weaken safeguards under the guise of efficiency.

*"I view all of this very critically, because under the broad term simplification – if we were living in a different world, I'd see it quite differently and say, great, let's take a look at that! But it's often more of a cover for dismantling regulation and, consequently, for weakening the protective*

*measures we have." (Jürgen Bering, Gesellschaft für Freiheitsrechte)*

Overall, these accounts highlight a shared recognition that regulatory harmonization is essential to making the AI Act workable in practice – but also a contested one. For companies, harmonization offers efficiency and predictability; for civil society, it raises concerns about weakening rights-based protections. The challenge lies in streamlining governance structures while preserving the normative commitments embedded in the EU's digital regulatory agenda.

Company representatives further emphasize that the regulatory process itself must evolve to keep pace with rapid developments in AI. They argue that the current pace and rigidity of EU lawmaking are misaligned with the fluid, iterative nature of AI innovation. Rather than treating regulation as a static framework, they call for a more adaptive legislative process that allows for continuous feedback and technical iteration as technologies advance.

*"The key issue is that legislation must respond as quickly as possible to technological change – especially in AI. Every two months, a new model comes out. Every six months, we have a new chip generation. And in that same time frame, legislators might have met three times – by which point we already have entirely new models and almost a different AI system altogether. I definitely see a need for improvement here." (SME, legal tech)*

Company representatives also emphasize the need stronger and more structured involvement of industry actors in regulatory design. They argue that meaningful participation by practitioners is essential to ensure that evolving rules remain grounded in technical realities and market dynamics. In their view, expert panels that combine scientific and practical expertise could help develop shared definitions and maintain relevance in fast-evolving areas such as generative or agentic AI.

At the same time, civil society representatives call for broader participation in these processes to ensure that the regulatory dialogue is not dominated by industry interests alone. They argue that public accountability and inclusiveness must remain central to any mechanism for adaptive governance, especially as definitions and classifications take on normative and political significance.

Some interviewees advocate for a more trust-based approach to compliance, arguing that excessive rigidity risks undermining both innovation and regulatory effectiveness. They suggest that the EU draw on mechanisms already in use – such as voluntary self-assessments, certification schemes or transparency tools – to encourage responsible behavior without imposing unwarranted administrative burdens.

*"More flexibility to the manufacturers because the law cannot predict every single use case and technology evolution. So, it needs to be somehow left to the common sense of the manufacturer, while providing principles for AI systems' safety. Also, they need to trust the manufacturers that they know what they do and their business depends on reliable and robust technology." (SAP)*

From this perspective, company representatives argue that effective regulation depends on cultivating a culture of trust between regulators and innovators.

At the same time, interviewees suggest that the AI Act should be refined rather than reopened or weakened. They emphasize the need for more nuanced regulation that enhances precision, accountability and protection without adding unnecessary complexity. One proposal involves introducing a more differentiated risk taxonomy – additional categories between limited-risk and high-risk systems – to better capture technological diversity and reduce excessive compliance burdens. Yet civil society representatives challenge this idea as "adding more complexity and legal uncertainty" (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie).

Civil society representatives call for stronger safeguards for fundamental rights by closing existing loopholes, particularly in relation to remote biomet-

ric identification (RBI). They stress that current exemptions – especially those permitting use by police, law enforcement and migration authorities – pose significant risks to fundamental rights.

> *"RBI [should be] [...] more strongly regulated ex post. The exemptions for state use – especially by police, law enforcement or in migration – are highly critical." (Jürgen Bering, Gesellschaft für Freiheitsrechte)*

From this perspective, the AI Act's legitimacy hinges on its ability to protect citizens from harmful uses of AI, not only in the private sector but also in the public sector. Rather than relying on a patchwork of exemptions, CSO representatives call for a clear baseline of disclosure that guarantees accountability.

> *"These kinds of exemptions are not justifiable. It would make much more sense to establish consistent transparency requirements for everyone and introduce a legal baseline – a minimum threshold of disclosure – that actors can always choose to exceed if they wish." (CSO)*

To this end, CSO representatives highlight the need for "strong and meaningful fundamental rights impact assessments" (CSO), supported by clear guidance and mechanisms for public accountability. They criticize what they view as the Commission's overly minimalist approach, warning that reducing compliance obligations too far risks rendering the exercise ineffective.

> *"The Commission is tasked with developing a questionnaire for fundamental rights impact assessments, but they're thinking about it in a very minimalist way – trying to avoid any additional compliance burden. But that makes it useless. In some countries, like the Netherlands, we already see more effective approaches. You need to provide good materials and clear guidance: What are the fundamental rights risks, how have I assessed them, and – most importantly – make this public. It must be traceable what fundamental rights risks I have considered. We are currently working with a group to develop a proposal for this." (CSO)*

Taken together, these proposals point to the gradual refinement of the AI Act into a more adaptive and practicable framework. Interviewees emphasize the importance of shaping the Act into a dynamic governance system – one that evolves with technological and societal change while strengthening protections without constraining innovation.

## C. Interim conclusion

The interviews reveal a broadly positive reception of the EU AI Act's objectives. Stakeholders recognize its potential to establish trustworthy and coherent AI governance, enhance legal certainty and protect against misuse. Yet concerns – particularly among companies – center on practical implementation, including the need for regulatory clarity, manageable administrative burdens and coordinated guidance supported by technical standards. Key priorities include simplifying horizontal and sector-specific requirements, harmonizing the wider EU digital regulatory landscape and clarifying responsibilities across the AI value chain. Civil society organizations likewise endorse the Act's ambition but warn against reopening or weakening its provisions. They call instead for stronger transparency, consistent accountability mechanisms and the closure of loopholes, especially in areas such as biometric surveillance. While corporate actors emphasize feasibility and operational practicality, civil society groups highlight democratic oversight and the protection of fundamental rights. Despite these differing emphases, there is broad agreement that the Act's success will depend on precise guidance, robust institutional support and the effective translation of legal principles into operational practice.

# III. Policy suggestions

As part of its "simplification" agenda, the European Commission has announced a digital omnibus package planned for late 2025 or early 2026, aimed at reducing bureaucratic reporting requirements for companies and harmonizing the digital regulatory framework, including European AI regulation and thus the AI Act. While some civil society representatives describe this initiative as opening Pandora's box, others – particularly industry participants – see it as an opportunity to incorporate practical implementation experience and adapt legislation to rapid technological change. In the following nine sections, we make targeted suggestions informed by the empirical findings.[2]

## 1. Prohibitions (Art. 5): Post-remote biometric identification

Article 5 prohibits AI practices deemed incompatible with Union values and includes detailed restrictions on real-time RBI in public spaces. Post-remote biometric identification (ex post RBI), however, receives only limited treatment through Article 26(10) and three nonbinding principles in Recital 95: proportionality, the prohibition of indiscriminate surveillance and the prevention of circumvention. This approach delegates substantive regulation to Member States and creates significant inconsistencies in an area central to fundamental rights protection in an era of expansive digital surveillance capabilities.

Article 26(10) requires authorization for post-remote biometric identification in law enforcement investigations, but it does not limit such deployments to serious crimes. Instead, the provision permits use for "a specific criminal offense," without adopting the gravity threshold outlined in Article 5 and Annex II, which restrict real-time biometric identification to serious offenses carrying substantial custodial penalties. Scholars have noted that post-event biometric searches can replicate many of the surveillance effects associated with real-time systems, since both can facilitate pervasive monitoring and deter participation in public life (Giannini & Tas, 2024; Gabrielli, 2025). This absnce of a seriousness criterion introduces a structural risk that biometric identification could be used to target conduct that, while criminalized domestically, remains protected under Union fundamental rights doctrine. For example, participation in a peaceful LGBTQ+ parade – behavior that certain national frameworks have treated as criminal, as discussed in analyses of restrictive assembly laws in Member States such as Hungary (Anderson, 2025) – illustrates this danger. Research further warns that expansive criminal triggers may chill expression and assembly, particularly among vulnerable groups (Warthon, 2023; Raposo, 2022), and that the AI Act grants broad discretion to Member States in ways that may lead to uneven levels of protection (Paolucci, 2024; Tracol, 2025). Evidence that AI systems can infer sensitive attributes such as sexual orientation from facial data underscores the stakes for minority communities (Wang & Kosinski, 2018). The absence

2 The authors note that the proposals and analysis sections of this study also draw on their own professional experience and judgment, which may extend beyond or diverge from the empirical findings. Any views expressed in these sections should therefore not be understood as representing the perspectives of the interview participants.

of a serious-crime limitation for post-remote biometric identification therefore constitutes a material deficiency that undermines effective and uniform protection of dignity, privacy, freedom of expression and freedom of assembly across the Union.

Notably, the GDPR and the Law Enforcement Directive (LED) do apply to such cases and already prohibit certain forms of ex post RBI (see European Commission, 2025, para. 429). Even so, both frameworks – like the AI Act – delegate core regulatory discretion to Member States. For example, Article 10(a) of the LED permits the use of biometric data on the basis of any "Member State law" that meets constitutional requirements, creating a notably permissive pathway. As a result, fundamental rights protections remain uneven across the Union.

The temporal distinction between real-time and ex post RBI also offers little meaningful protection in practice. Law enforcement authorities can simply record public spaces continuously and apply biometric identification days later, achieving the same surveillance effects while avoiding the restrictions of Article 5. Civil society organizations interviewed for this study stressed that applying facial recognition to footage of demonstrations days after the fact produces the same chilling effects on democratic participation as real-time processing. Citizens cannot know whether lawful participation in public life will expose them to future surveillance-based consequences.

Delegating ex post RBI regulation to Member States leads to predictable problems. Countries with strong rule-of-law traditions may implement robust safeguards, while others – particularly those experiencing democratic backsliding – may exploit the regulatory gap to expand surveillance practices, as initial reports suggest (Anderson, 2025). This inconsistency leaves the protection of citizens' fundamental rights dependent on geography rather than harmonized EU standards.

Given these risks, Article 5 could explicitly prohibit ex post RBI in publicly accessible spaces for law enforcement purposes, mirroring the restrictions placed on real-time RBI. Narrow exceptions could be maintained, but only in parallel with those governing real-time RBI – allowing use solely in cases involving severe crimes listed in Annex II and only by police or other competent law enforcement authorities.

## 2. High-risk provider regulation (Art. 6-24 AIA): Toward a more sectoral approach

The interviews suggest two avenues for shifting the AI Act toward a more sector-tailored structure. First, certain items could be removed from Annex III and incorporated into dedicated sectoral instruments in areas such as employment, creditworthiness assessment and insurance supervision. Second, it may be useful to subject sectors already governed by existing regulatory frameworks to corresponding sector-specific revisions, which would require reclassifying them from Annex I A to Annex I B. The sole consequence of such a shift would be that regimes currently listed under Annex I A would fall outside the direct scope of the AI Act and would instead require explicit modernization by a fixed deadline – for example, Aug. 2, 2028. Interviews and workshop discussions indicate that human oversight is the central theme most in need of such adaptation. Any sector that fails to implement an AI-relevant amendment by Aug. 2, 2028 would automatically revert to Annex I A, ensuring continued AI-specific coverage. It is therefore essential that such updates not be deferred indefinitely or risk leaving some sectors without necessary alignment.

With these caveats in mind, this section proposes targeted removals from the high-risk category and advocates for sector-specific regulatory approaches in two key areas: Annex III (employment and finance); and Annex I A (New Legislative Framework sectors).

### a) New high-risk sectors (Annex III)

Annex III of the AI Act identifies several high-risk sectors – including employment, credit scoring and

insurance – that, while generally regulated, have not previously been part of the EU's specific product safety regime. We begin with these domains.

### i. Employment

The employment sector presents the strongest case for removal from Annex III. This is not because workplace AI systems pose minimal risks – on the contrary, they present significant and specific risks to affected individuals. Rather, their regulation could be shifted into a dedicated directive on AI in the workplace.

Recent discussions in the European Parliament indicate growing legislative support for this approach. A dedicated instrument would interface more effectively with the Platform Work Directive (PWD) and help eliminate contradictions between the two frameworks. For instance, while the AI Act prohibits emotion recognition in the workplace but allows it for medical or safety reasons, the PWD lacks a corresponding exemption. These rules and their exceptions should be harmonized.

Furthermore, Article 114(2) TFEU creates constitutional barriers to the current framework by explicitly excluding "provisions relating to the rights and interests of employed persons" from internal market harmonization under Article 114(1) – the legal basis of the AI Act's employment provisions (see Recital 3 AIA). As a result, specific worker-rights provisions in the Act (Articles 26(7) and 85–86) risk falling outside the permissible scope of Article 114(1), potentially violating Article 114(2). In other words, several employment-related rules in the AI Act may no longer qualify as product regulation ***strictu sensu*** and thus exceed the Act's legal basis.

A separate directive passed under Article 153 TFEU would resolve these constitutional concerns and ensure proper consultation with social partners, as required by EU social policy procedures under Article 154 TFEU. Such a participatory process would likely yield a more balanced and effective framework – one that reflects the distinct dynamics of employment relationships and aligns more coherently with existing and forthcoming labor law initiatives, including the Platform Work Directive.

### ii. Credit scoring and insurance

Credit scoring and insurance applications likewise merit removal from the high-risk category in Annex III. These sectors already operate under comprehensive regulatory frameworks that govern algorithmic decision-making and risk management. Existing credit scoring rules and financial services directives create overlapping – and at times duplicative – requirements alongside those in the AI Act. Recent scholarship demonstrates that this redundancy imposes compliance burdens without delivering meaningful gains in consumer protection (Cordes & Hacker, 2025; Hacker, 2024; Hacker & Eber, 2025; Mazzini & Bagni, 2023; see also Spindler, 2021; Langenbucher, 2020, 2022; Hacker & Passoth, 2020). The banking and insurance sectors have developed mandatory and sophisticated risk management protocols for validating AI systems, many of which exceed the AI Act's horizontal requirements in granularity and rigor. These sector-specific frameworks offer more nuanced and effective governance mechanisms than the AI Act's more general, cross-sector approach.

Financial institutions face substantial challenges in determining which horizontal AI Act requirements exceed their existing regulatory obligations and therefore require additional compliance measures beyond established sectoral rules.

In this landscape, Article 17(4) stands out as a rare example of successful regulatory integration. It allows financial institutions to rely on governance systems established under frameworks such as CRD IV to meet the AI Act's quality management requirements. The provision recognizes that Union financial services legislation already mandates equivalent controls in areas such as risk management and compliance oversight. Institutions may therefore satisfy the AI Act's quality management obligations through existing mechanisms. However, this integration remains limited. Article 17(4) explicitly excludes

post-market surveillance, incident notification and documentation protocols. These areas constitute distinct AI Act obligations that financial institutions must implement through separate operational processes. The delineation provides valuable clarity by identifying where additional AI Act compliance is required beyond existing sectoral rules (Hacker, 2024; Hacker & Eber, 2025; see also Langenbucher, 2020).

The scope of Article 17(4) reveals a critical limitation: the integration mechanism applies only to quality management systems. It offers no guidance for reconciling other AI Act requirements with sectoral frameworks. Articles 9 through 15 impose extensive obligations relating to risk management, data governance, technical documentation, record-keeping, transparency, human oversight and accuracy. Financial institutions must navigate these requirements without clear instructions on how they align with parallel duties under banking, insurance and securities regulation (Cordes & Hacker, 2025). This regulatory gap forces institutions to maintain potentially duplicative compliance structures. The absence of comprehensive integration provisions across all AI Act requirements undermines regulatory efficiency and creates unnecessary compliance burdens.

If credit scoring and insurance remain in Annex III, the financial sector will require integration mechanisms that extend well beyond quality management to cover the full spectrum of AI Act obligations. Financial service providers and insurers currently face the difficult task of mapping overlaps between the AI Act and existing frameworks, including the credit scoring provisions in Articles 142 et seq. of the Capital Requirements Regulation, nondiscrimination rules such as Section 19 of the German General Equal Treatment Act, and sectoral administrative instruments such as the AI validation requirements under MaRisk (Minimum Requirements for Risk Management), particularly AT 4.3.5. A comprehensive analysis of MaRisk reveals extensive duplication of regulatory requirements (see, for example, Cordes & Hacker, 2025). Without such comprehensive alignment, credit scoring and insurance applications will continue to face overlapping and potentially conflicting regulatory obligations that neither strengthen consumer protection nor foster innovation.

Conversely, a targeted removal of these cases from Annex III would streamline the scope of the AI Act while preserving strong protections through existing sectoral frameworks. Crucially, by updating sector-specific regulations in areas where the AI Act goes beyond current rules – for instance, the human oversight provisions in Article 14 – the fundamental rights and interests of affected persons would remain fully safeguarded.

## b) Toward more sectoral rules: From an annex I A to an annex I B logic

The current bifurcation between Annex I A and Annex I B in the AI Act creates an artificial regulatory divide that complicates coherent AI governance. Annex I A places products already regulated under the New Legislative Framework (NLF) – such as medical devices, machinery and toys – under the direct application of the AI Act. Annex I B, by contrast, requires sectors governed by legislation under the Old Legislative Framework (OLF) – including automotive, transportation and aviation – to incorporate AI Act principles through subsequent regulatory updates. This distinction lacks substantive justification and produces significant implementation challenges.

A core question therefore arises: should all AI applications currently covered under Annex I A transition to an Annex I B model? Under such an approach, these sectors would fall outside the direct scope of the AI Act and would instead be required to update their respective sectoral regulations to incorporate relevant AI governance principles.

### i. Healthcare

Healthcare illustrates these structural challenges particularly clearly. Medical AI systems face duplicative requirements under both the AI Act and the Medical Device Regulation (MDR). The MDR already sets out comprehensive safety and performance require-

ments for software as a medical device. Adding a parallel layer of AI Act obligations introduces compliance complexity without delivering clear safety benefits (see Yeung, 2025, pp. 14–17, for comparison of risk management alone). For example, Article 15(1) of the AI Act requires medical AI systems to demonstrate appropriate "accuracy." Yet accuracy is widely regarded as a misleading performance metric in medical contexts (Hicks et al., 2022). Reflecting this, the MDR mandates a rigorous clinical evaluation process and a positive benefit–risk ratio (Articles 61 and 2(24), as well as Annex I, including Sections 1 and 8; see also Medical Device Coordination Group, 2020), rather than relying on a simplistic accuracy rate. Interviewees also raised concerns about the sequencing of CE marking – specifically, whether it should occur before or after clinical trials – and about how substantial modifications to AI-enabled medical devices should be handled, including when additional conformity assessments are required.

Recent developments in agentic AI systems, as analyzed in Freyer et al. (2025), underscore how rapidly evolving medical AI capabilities require flexible and sector-specific regulatory responses. The MDR's established mechanisms for clinical evaluation and post-market surveillance offer a more appropriate foundation for governing these emerging technologies than the AI Act's generic horizontal requirements. Updating the MDR with targeted AI-specific provisions would enable more precise and sector-informed regulation grounded in medical expertise and tailored to patient safety priorities.

### ii. Machinery

Manufacturing presents parallel challenges. The overlap between AI Act requirements and the new Machinery Regulation (MR) creates significant difficulties for AI-enabled industrial systems (Giovannone, 2025). The MR already embeds safety requirements for autonomous and AI-driven machinery and addresses the specific risks associated with industrial applications through established conformity assessment procedures. Layering additional AI Act obligations on top of this calibrated sectoral framework introduces unnecessary complexity. Manufacturers must navigate potentially conflicting technical standards and documentation requirements without a clear hierarchy or defined integration mechanisms. Unlike the financial sector, there is no provision analogous to Article 17(4) of the AI Act that would allow regulated entities to rely on existing governance structures (Hacker, 2024). As a result, it remains unclear which – if any – additional AI Act obligations manufacturers must fulfill beyond those stipulated in the MR.

### iii. From Annex I A to I B

The implementation challenges emerging across Annex I A sectors highlight the limitations of applying horizontal AI rules to products already governed under the NLF. These difficulties suggest that removing such sectors from direct AI Act application – and instead requiring targeted adaptations of sectoral market access regulations – would yield more effective and coherent governance. Moving toward an Annex I B approach across all NLF sectors would establish a more consistent regulatory philosophy: for sectors already subject to product safety legislation, the AI Act would operate as a framework instrument that mandates sector-specific updates rather than imposing direct horizontal obligations.

In this model, the revised AI Act would need to clarify that existing harmonized standards under the NLF remain in force and that the NLF logic continues to apply uninterrupted. The only change would be that NLF legislation would no longer intersect directly with the AI Act but would instead be subject to mandatory updates by a fixed deadline – for example, August 2028. Based on our interviews and workshop discussions, these updates would primarily concern human oversight requirements. If a sector fails to implement the necessary AI-relevant update by August 2, 2028, it would automatically revert to Annex I A to ensure continued AI-specific coverage. This model, in our view, better reflects sectoral expertise, reduces regulatory fragmentation and enables more tailored responses to AI-related risks within specific domains. Legislative bodies would retain clear obligations to

align sectoral regulations with AI Act principles, but implementation would occur through established sectoral channels – drawing on familiar stakeholder engagement processes and existing technical standardization structures.

## c) Data and data governance (Art. 10)

The AI Act's data governance regime in Article 10 could be restructured to prevent the creation of conflicting standards with existing nondiscrimination law while enabling effective bias mitigation. Four reforms appear particularly useful (see also Hacker, 2021; Van Bekkum, 2025).

First, Article 10 could reflect the limited applicability of nondiscrimination law to mere data-curation activities (see Kilian/Schefzig, 2025, para. 15). As the Court of Justice clarified in ***Associazione Avvocatura per i diritti LGBTI*** and ***Feryn***,[3] EU nondiscrimination law extends to preparatory activities only when specific criteria are met: a concrete link to protected activities, decisive influence on outcomes and sufficient publicity. The internal compilation of training data for general-purpose AI models will often not meet these criteria (Hacker, 2021). Once such models are deployed in high-risk settings, however, Article 10 applies by virtue of Article 25(1)(c).

Article 10's references to bias detection and mitigation can therefore be misleading, as they imply that nondiscrimination law automatically governs all data-curation activities. For instance, Article 10(2)(f) requires an "examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law [...]." This creates a misalignment that forces developers to navigate between Article 10's requirements and nondiscrimination law's actual scope.

The provision could therefore clarify that its requirements establish independent data-quality standards that complement – rather than duplicate – nondiscrimination law. Where nondiscrimination law does apply (for example, when data is compiled specifically for employment screening), Article 10 could explicitly defer to those established frameworks. Where it likely does not apply (for example, in general-purpose data collection, see Hacker, 2021), it may be more appropriate for Article 10 to provide clear, standalone quality criteria without invoking nondiscrimination obligations that lack a solid legal basis. Such criteria could include, where feasible, measures of dataset composition and balance.

Second, the exception in Article 10(5) allowing the processing of sensitive data for bias detection and correction requires both material and temporal expansion. Currently limited to high-risk systems, the exception fails to reflect that meaningful bias mitigation benefits all AI applications. Low-risk systems can still produce discriminatory outcomes, and restricting access to debiasing tools creates a perverse incentive: developers may avoid bias testing altogether for fear of violating Article 9 GDPR (cf. Van Bekkum & Zuiderveen Borgesius, 2023). For this reason, the Article 10(5) exception could apply to all AI systems where developers can demonstrate a genuine bias-mitigation purpose.

More critically, the provision in Article 10(5) must apply before the general obligations of Article 10 take effect. As written, the provision creates a temporal paradox: developers may use sensitive data for debiasing only after their systems are already required to comply with Article 10. This defeats the purpose of enabling proactive bias mitigation during the year preceding the application of the high-risk rules. The provision could therefore state explicitly that processing for bias assessment and mitigation may begin during system development, before market placement, and before the current August 2, 2026 deadline.

Third, it is essential to clarify that Article 10(5) provides only a derogation from Article 9 GDPR's prohibition on processing sensitive data, and does not constitute an independent legal basis under Article 6 GDPR (Kilian/Schefzig, 2025, para. 68; cf. also Van

3 CJEU, Case C-507/18, Associazione Avvocatura per i diritti LGBTI; Case C-54/07, Feryn.

Bekkum, 2025). The current drafting risks misleading developers into assuming that Article 10(5) alone authorizes sensitive-data processing.

To avoid ambiguity, the text would benefit from making clear that developers need a valid legal basis under Article 6 GDPR – typically legitimate interests under Article 6(1)(f) – and that Article 10(5) functions only to lift Article 9's categorical prohibition.

Finally, Article 10 could acknowledge that effective bias mitigation may require in-processing or post-processing interventions, rather than modifications to the training data. Research shows that certain fairness constraints can be achieved more efficiently and reliably through output-level adjustments than through dataset rebalancing. Mandating data-level interventions where superior technical solutions exist imposes unnecessary burdens without improving outcomes. Article 10 could therefore adopt an outcome-oriented approach that allows developers to select intervention methods appropriate to the model architecture, provided they demonstrate effective bias reduction. At a minimum, the Act would benefit from including a defense allowing providers to show that any residual dataset imbalances were effectively mitigated at later stages of the machine-learning pipeline (Hacker, 2021).

### d) Accuracy and performance (Art. 15)

Article 15's requirement for "an appropriate level of accuracy" misconstrues how AI system performance should be evaluated. Addressing this would involve amending the provision to require "appropriate performance," measured through context-appropriate metrics, since accuracy alone often fails to capture critical system behavior and can even incentivize harmful outcomes. This adjustment must be applied consistently across both Article 15(1) and Annex IV, which likewise privileges accuracy at the expense of more meaningful performance indicators.

Accuracy is an inadequate universal metric across a wide range of AI applications. Whenever events are rare, classes are imbalanced, or errors carry asymmetric consequences, accuracy can be actively misleading (Lindholm et al., 2022, p. 86 et seqq.). In medical diagnosis, for example, a system achieving 99% accuracy by labeling all patients as healthy would be catastrophically unsafe despite its impressive score (Hicks et al., 2024). What matters instead is sensitivity (capturing actual cases) and specificity (avoiding false alarms), with the optimal balance dependent on disease severity and the risks of delayed treatment. Similarly, in credit scoring, accuracy tells us nothing about whether a model exhibits discriminatory lending patterns (Langenbucher, 2020). Fairness metrics – such as demographic parity or equalized odds – capture harms that accuracy simply ignores.

Fraud detection systems illustrate the same flaw: when fraudulent transactions account for less than 1% of activity, a model predicting no fraud achieves 99% accuracy while providing zero value. Precision and recall offer far more meaningful measures of performance when it comes to capturing the system's ability to identify actual fraud while minimizing false positives that inconvenience legitimate customers. Recommendation systems also demonstrate the limits of accuracy. Predicting user clicks does not capture whether the system promotes content diversity, avoids filter bubbles or supports user well-being. Metrics such as coverage, novelty and long-term user satisfaction prove more relevant in practice. Natural language processing applications demonstrate similar limitations: high word-level translation accuracy can coexist with incoherent output. Bilingual Evaluation Understudy (BLEU) scores, semantic similarity measures and human evaluation provide a more reliable picture of translation quality.

### e) Post-market monitoring (Art. 72)

Article 72 regulates post-market monitoring by providers and requires a dedicated post-market monitoring plan for all high-risk AI systems. The provision is designed to establish a basis for evaluating high-risk systems once they are placed on the market

and can be understood as a temporal extension of Article 9 (see Rec. 155). It applies across the "entire life cycle" of the system and addresses providers, while indirectly imposing related duties on deployers.

Under Article 72(3), the monitoring system must be built on a formal monitoring plan, which becomes part of the system's technical documentation. The European Commission is tasked with specifying the detailed provisions for developing this plan – along with the list of required elements – through an implementing act.

### i. Inflexibility

In general, the legislative choice to provide both a template for the post-market monitoring plan and a corresponding list of required elements is broadly welcomed. These tools help translate otherwise abstract legal obligations into concrete, usable guidance and reduce implementation burdens – particularly for SMEs and startups.

Because Article 72 explicitly requires post-market monitoring systems to be proportionate to the nature of the AI technology and the risks posed by a given high-risk system, it will be essential to ensure that the needs and constraints of SMEs are properly reflected in both interpretation and enforcement. In any case, it remains an open question as to whether the implementing act adequately reflects this proportionality.

### ii. Temporal aspects

Uncertainties arise from the fact that the implementing act does not need to be finalized until February 2, 2026 (see also Djeffal, 2025, para. 31). Because Article 72 becomes applicable on August 2, 2026 under Article 113, sentence 2, providers will have only six months to develop post-market monitoring plans that comply with the implementing act. This leaves a significant transitional period – up to February 2, 2026 – during which organizations lack clarity on how such plans should be designed. In addition, the six-month window for implementation appears insufficient for many actors to operationalize these requirements, particularly given the complexity of post-market monitoring obligations. This concern is partly addressed by the adjustment of the application date in Article 113, sentence 2 (see Article 113).

## f) Compliant AI systems that present a risk (Art. 82)

Article 82 authorizes market surveillance authorities to require an operator to take appropriate corrective measures if a high-risk AI system – despite formally complying with the AI Act – still poses a risk to health or safety, to fundamental rights or to other aspects of public-interest protection.

According to Article 74(4), Article 82 does not apply where equivalent sector-specific procedural rules already exist for AI systems associated with products listed in Annex I, Section A. This includes, for example, Article 45 of the Machinery Directive (Machinery Directive).

In the absence of legislative clarification in the recitals, the scope of this exemption remains unclear. This ambiguity creates understandable uncertainty for regulated entities.

While some scholars argue for a broad reading of Article 82 based on its open wording (Hartmann, 2024, para. 10), the provision is better interpreted narrowly and proportionately. On this view, only those public interests form the prerequisite or foundation for the protection of the rights and interests expressly listed in the provision should qualify as grounds for intervention (Djeffal, 2025, para. 23). This may include aspects of the rule of law, democratic integrity or environmental protection – provided a clear and specific connection exists to health, safety or fundamental rights.

This narrower reading is consistent with the ejusdem generis principle. The principle states that when legislation mentions specific terms followed by a general clause, the scope of the general clause is limited

to subjects comparable to those specifically enumerated. It provides for a restriction to protected goods that are comparable to those expressly mentioned (MacKay, 1920). Following, the term of „other aspects of public interest protection“ in Article 82(1) has to be interpreted in the light of „a risk to the health or safety of persons“ and „(a risk) to fundamental rights“. Any other interpretation would carry the risk of unlimited application, thereby increasing legal uncertainty and undermining the effectiveness of the provision.

In addition, Article 79(1), read together with Article 3(1) of Regulation (EU) 2019/1020, clarifies that a "risk" under Article 82(1) exists only when the protected interests are affected to a degree that exceeds what is considered reasonable and acceptable in relation to the system's intended purpose (...). Therefore, not every conceivable risk is sufficient. Although restrictive interpretation can mitigate some of the provision's vagueness, it still leaves operators facing significant legal uncertainty. For this reason, a more explicit clarification of the phrase "other aspects of public interest protection, which are the prerequisite and basis for the protection of the aforementioned" would be highly desirable

## 3. High-risk deployer regulation

### a) Obligations of deployers of high-risk AI systems (Art. 26)

Article 26 sets out specific obligations for deployers of high-risk AI systems. Among other requirements, deployers must take appropriate technical and organizational measures to ensure the system is used in line with the accompanying instructions and with paragraphs 3 and 6; designate a qualified natural person with the requisite competence to exercise human oversight; and comply with specific monitoring, reporting and documentation obligations. Other obligations of the deployers remain unaffected.

From a legal standpoint, the monitoring duties under Article 26(5) raise questions – not because monitoring is unnecessary, but because comparable obligations already arise under tort law whenever deployers use or control a product (see also Mantelero, 2024). Such obligations are traditionally justified by the deployer's presumed superior knowledge and factual control during operation, which enables preventable harms to be avoided (see Recital 93, sentence 3; Denga, 2025, para. 52). Yet it is at least debatable whether deployers consistently hold this informational or operational advantage in AI practice. In some contexts, providers may actually be better positioned to exert meaningful oversight or exercise technical control over system behavior.

More importantly, the added value of the monitoring obligation remains unclear. An analysis of tort law, including the Product Liability Directive (PLD) and national tort regimes, shows that deployers are already required to monitor their systems in agile, context-specific ways. Where the deployer is also the manufacturer, the revised PLD already captures these scenarios. Article 7(1)(e) PLD now makes explicit that product defects may arise while the manufacturer retains control over the product after it has been placed on the market – that is, during deployment – and Article 7(1)(c) extends responsibility to harms caused by an AI system's capacity to learn during use (Art. 7(1)(c) PLD In cases where the deployer is not the manufacturer, the PLD's scope is more limited, but national tort law fills much of this gap. It covers additional categories of harm, including discrimination, defamation, and libel (Wagner, 2023; Hacker et al., 2025). Crucially, tort law applies to all actors along the value chain; national tort rules remain applicable even when an actor is already subject to PLD obligations (Art. 2(4)(b) PLD).

Dogmatically, national tort law – particularly in European jurisdictions – draws on well-established principles. Its central point of reference is a breach of the relevant duty of care by the actor in question, which must have caused both the infringement of legally protected interests and the resulting damage (Green, 2001). In certain circumstances, strict liability

regimes also apply (Hacker et al., 2025). As a general rule, any actor using potentially harmful products must take all reasonable precautions to prevent harm to third parties. These obligations include monitoring duties, which extend to the deployment of AI systems (see, in detail, Wagner, 2024, para. 890).

That tort law can function effectively as a mechanism of oversight is illustrated by the German Federal Court of Justice's "autocomplete" decision.[4] In 2013, the Court held Google – acting simultaneously as provider and deployer – liable for defamatory autocomplete suggestions produced by its search engine (Smith, 2013). The ruling makes clear that if developers fail to implement adequate safeguards or neglect to act upon notification of harmful outputs, they may incur liability for violations of personality rights or comparable interests (Hacker et. al., 2025). However, this finding is not limited to providers of AI systems. It applies equally to deployers, because tort law addresses all actors in the chain of causation. Accordingly, under prevailing tort law doctrine, each party along the AI value chain is required to do whatever is possible, reasonable and appropriate – given its level of control over the system and its outputs – to prevent harm (Hacker & Holweg, 2025).

This demonstrates that tort law, through general principles, already encompasses the underlying rationale of Article 26(5) and recognizes that risks may arise not only from the design of an AI system but also from how it is used (Recital 93, sentence 1). Under tort law, the obligation to exercise appropriate control over a deployed system inherently includes a duty to monitor – functionally mirroring the monitoring requirement in Article 26.

However, while tort law lacks a public enforcement apparatus, it is considerably more flexible because it relies on general standards rather than rigid legal obligations. Instead of hinging on whether an AI system is classified as "high-risk," tort law applies to all AI models and systems and evaluates conduct based on the specific circumstances of each case. In this respect, tort law arguably reflects the principle of proportionality more effectively than the AI Act's categorical framework – an approach that should, in principle, inform the Act's risk-based logic.

This point becomes particularly salient when considering Article 26(5), second sentence, which obliges deployers to suspend use of a system if there is reason to assume it poses a risk. Under the AI Act, use must be halted whenever the system presents a risk to "the health or safety, or to fundamental rights, of persons" that exceeds what is considered "reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use" (Art. 3(19) of Regulation (EU) 2019/1020, read together with Article 79(1); see also Article 25(5)(2) and Denga, 2025, para. 48).

Again, the obligation to suspend the use of an unsafe AI system would arise under general tort law as well, provided the risk is sufficiently serious. This is a reasonable standard. Yet under tort law, if the risk threshold is met, the duty applies not only to deployers of high-risk AI systems but to deployers of any AI system. Conversely, if the risk is insufficient, even deployers of high-risk systems would not be required to suspend use across the board.

Beyond offering increased flexibility, the application of general tort law provides a high degree of legal clarity grounded in decades of jurisprudence. Both deployers and courts are already accustomed to applying product liability and tort principles. This avoids the misconception that monitoring obligations are a novel requirement with undefined standards. Instead, it reinforces that the relevant principles are well established and have long guided judicial assessments, as demonstrated by existing case law (see above).

Industry interviews reveal significant practical concerns about Article 26. One AI provider reported: "We see that people are really less willing, and you have to really take away their fear… especially with Article 26, that the deployers themselves have to ensure that their data is appropriate for what they use it for, that they need instructions on how to use it."

4 BGH, Case VI ZR 269/12, Judgment of May 14, 2013.

The provider explained that they proactively clarify the meaning of Article 26 and outline where they can offer support, yet apprehension remains widespread in the market. A representative of a large industrial company managing more than 4,000 applications voiced similar concerns: "The fact that we say I'm evaluating an AI system, but we see that in the future almost everything will be AI systems. (...) This means for us that we also have corresponding obligations as operators there, and fulfilling these obligations – can you imagine what an insane administrative effort that is?"

These theoretical and practical considerations together suggest that the monitoring obligations in Article 26 could be removed insofar as they do not add independent regulatory substance. Where monitoring and suspension duties already arise under tort law, Article 26 merely duplicates existing obligations. The result is an additional regulatory burden, particularly in sales processes, where AI providers encounter contractual partners who fear being drawn into a high-maintenance compliance regime with a questionable cost-benefit ratio. By contrast, the specific information duties in Article 26(5)(3–4) constitute a meaningful warning mechanism and could appropriately remain in place.

## b) Fundamental rights impact assessment for high-risk AI systems (Art. 27)

Article 27 requires certain deployers of high-risk AI systems to conduct a fundamental rights impact assessment (FRIA) (see, e.g., Mantelero, 2024). The obligation applies, first, to deployers that are bodies governed by public law or private entities providing public services. It also extends to "deployers of high-risk AI systems referred to in points 5(b) and (c) of Annex III," meaning private actors involved in credit scoring and certain insurance activities. The purpose of this requirement – ensuring effective protection of fundamental rights (Recital 91) – is welcome in principle and aligns with a broader trend in recent European regulation toward embedding ex ante rights-based assessments (see Denga, 2021).

### i. Private deployers as suitable addressees

A threshold question concerns the extent to which private actors can be subject to fundamental rights obligations in the first place (see, e.g., Auer, 2025). The primary benchmark is the Charter of Fundamental Rights of the European Union (CFR) (Art. 51(1) sentence 1 CFR; see Kingreen, 2022, para. 8; Yeung, 2025, pp. 23–24). One might argue that for deployers to have an "impact on fundamental rights" within the meaning of Article 27(1), they must themselves be bound by these rights. The issue, therefore, is not one of indirect third-party effects in private-law relationships but of the direct binding force of fundamental rights on private entities.

According to the Court of Justice of the European Union (CJEU), private individuals are directly bound by fundamental rights only in relation to certain equality and social rights (Ciacchi, 2018). Fundamental rights relating to individual freedoms do not appear in this line of case law[5] (for a critical view, see Fornasier, 2015).

A direct binding effect would require that the relevant provision of the CFR be sufficiently specific and contain clear indications of direct applicability to private actors. This is arguably the case only where the protected interests are primarily threatened by private conduct (see, e.g., Kingreen, 2022, para. 24). Furthermore, the binding nature of fundamental rights on private entities is typically confined to asymmetrical relationships (e.g., Jarass, 2021, para. 42). In abstract terms: the greater the power imbalance, the stronger the justification for subjecting private actors to fundamental right duties (Denga, 2025, para. 27).

Following from this, the legislator appears to treat credit scoring and insurance deployers as if they were assuming a quasi-public role. Yet the Act offers no explicit justification. Recital 96 does not explain why these private deployers should be directly bound by fundamental rights. Instead, it only elab-

5 See Art. 21(1) and Art. 31(2) CFR; CJEU, Case C-414/16 (Egenberger); C- 68/17 (IR); Joined Cases C-569/16 and C-570/16 (Bauer and Willmeroth).

orates on situations in which "services that are important for individuals and are of a public nature can also be provided by private institutions," which refers to a different part of Article 27 – namely private entities performing public services. The recital does not address why credit scoring and insurance deployers are singled out, while other private actors with comparable discrimination risks – for example in housing or certain medical contexts – are not.

Recital 58, which outlines the logic behind the high-risk classification, provides a partial indication. It emphasizes that credit scoring and insurance constitute private services that are *"necessary for people to fully participate in society or to improve one's standard of living."* The AI systems deployed have a particularly strong impact on the lives of the data subjects (Hilgendorf & Härtlein, 2025, para. 3).

Recital 58 highlights these sectors' heightened potential for discrimination: ("lead to serious consequences for people's life and health, including financial exclusion and discrimination"; "may lead to discrimination between persons or groups and may perpetuate historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts"). Read together with Article 27, the most plausible interpretation is that the legislator grounds the direct binding effect of fundamental rights – at least implicitly – in this heightened risk of discriminatory outcomes. With respect to the specific right to nondiscrimination under Article 21 CFR, such reasoning is defensible: the Court of Justice of the European Union (CJEU) has recognized that Article 21 can bind private individuals directly.

However, this legislative approach ignores the fact that this direct effect is exceptional and applies only to specific fundamental rights (e.g., nondiscrimination). Article 27, by contrast, requires deployers to conduct an assessment covering all potentially affected fundamental rights. The deployed AI systems may implicate a wide range of fundamental rights that cannot be conclusively determined (see list in Rec. 48, for detailed analyses, see Seitz, 2024; for a measurement approach, see Malgieri & Santos, 2025). But extending the direct effect of all relevant fundamental rights to private entities appears to run squarely against Article 51(1) CFR.

Furthermore, at a minimum, Article 27 should clarify that private deployers may invoke fundamental rights themselves (e.g., Jarass, 2021, para. 43). Any balancing of conflicting fundamental rights could then be incorporated into Article 27 as part of the "assessment of the impact."

Accordingly, it is proposed to align the language of Article 27 more closely with the risk management obligation under Article 9. Article 9 ensures effective protection of affected persons through a provider-level risk management system,[6] wand the assessment of impacts on fundamental rights already forms part of the conformity assessment under that provision (Mantelero, 2024). Aligning the wording of Article 27 with Article 9 – for example, by requiring deployers to conduct a risk assessment concerning interests protected by fundamental rights – would preserve the provision's protective purpose. It would also bring Article 27 into closer coherence with the other categories of deployers it governs, namely ("deployers that are bodies governed by public law, or are private entities providing public services").

### ii. Equality

Even more importantly, imposing an obligation on private credit scoring and insurance deployers appears difficult to justify under the principle of equality, as enshrined in Article 20 CFR. Unequal treatment of essentially equal things or equal treatment of essentially unequal things is, therefore, only permissible if it is objectively justified and proportionate[7] (e.g., Ross, 2022, para. 20).

6 Granted, Article 9(2) sentence 2(a) also calls for identifying and analysing risks to "fundamental rights," which means that, strictly speaking, the same doctrinal complications arise here as well.

7 See CJEU, Case C-21/10 (Nagy).

Article 27 might prescribe the different treatment of fundamentally comparable entities by imposing obligations on credit scoring and insurance deployers but not on other private high-risk deployers.

A general requirement to conduct impact assessments, as foreseen in Article 27, could be justified with reference to the particularly significant effects that decisions by credit scoring and insurance deployers have on individuals' lives, as well as their heightened discrimination risks (Hilgendorf/Härtlein, 2025, para. 3; Rec. 58). Ensuring early and comprehensive mitigation of particularly serious risks is no doubt a legitimate and welcome goal.

However, it is unclear why banks and insurers – but not other providers – should be singled out, given that other high-risk use cases also carry substantial discrimination risks. For instance, the HR sector (Annex III, No. 4) makes decisions on "the selection of natural persons; promotion or termination of work-related contractual relationships" and, therefore, exhibits a similarly pronounced potential for discrimination. From an equality perspective, this suggests that either all or none of the private entities should fall under Article 27.

### iii. Effectiveness of Article 27

Finally, apart from these doctrinal foundations, questions arise about the practical effectiveness of the FRIA. Core challenges concern how to meaningfully assess interferences with fundamental rights (Malgieri/Santos, 2025). The omission of explicit references to potential elements of the FRIA from the final text of Article 27 may also make compliance more difficult for deployers (Mantelero, 2024).

While more ambitious formats are feasible (Kaminski & Malgieri, 2024), in practice the assessment will likely take the form of a questionnaire supported by automated tools. This approach risks devolving into a box-ticking exercise with limited substantive impact (Yeung, 2025, p. 6). Stakeholder participation seems only partially reflected in Article 27 (see Mantelero, 2024). Therefore, if left unrevised, the provision risks becoming a paper tiger that imposes costs and administrative burdens on deployers without significantly strengthening fundamental-rights protection.

### iv. Suggestions

Against this backdrop, clarifying Article 27 appears necessary. The obligation imposed on private deployers to comply with fundamental rights is doctrinally uncertain, and singling out credit scoring and insurance deployers is difficult to justify under equality principles.

It would therefore be beneficial to align Article 27 linguistically with the risk management obligations under Article 9 (see, for a discussion of risk-management approaches to fundamental rights, Yeung, 2025, p. 19 et seq.). Furthermore, the unequal treatment of private credit scoring and insurance deployers could be addressed. Finally, it remains to be seen whether Article 27 will meaningfully enhance fundamental-rights protection or function merely as a formal compliance exercise.

## 4. GPAI provider regulation

While a larger re-arrangement of GPAI provider rules appears unlikely at this stage (though see Hacker, Kasirzadeh and Edwards, 2025 for proposals), updates to the open-source rules and the Code of Practice would be advisable to foster effective AI uptake and compliance.

### a) Open-source AI models and systems

In the context of open source, we examine both the definition itself and the transparency requirements needed to help downstream developers comply and to allow society to better assess AI's climate impacts.

### i. The definition problem

The EU AI Act currently lacks a coherent definition of open-source AI. Article 53(2) defines open source for

the purposes of GPAI regulation as applying to "providers of AI models that are released under a free and open-source license that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available." By contrast, Article 2(12) uses different language: "This Regulation does not apply to AI systems released under free and open-source licenses."

This inconsistency creates legal uncertainty. A more coherent approach would involve adopting a uniform definition of open source models and systems in Article 3, with Article 53(2)'s definition governing open-source AI models. For open source AI systems, a parallel definition could read: "AI systems released under free and open-source licenses that allow for the access, usage, modification, and distribution of the system, and whose information on system usage is made publicly available." This formulation acknowledges that information on parameters may not be available when an open-source AI system relies on a proprietary underlying model. For consistency, Article 25(4) could mirror this language: "making accessible to the public tools, services, processes or components, other than general-purpose AI models, under a free and open-source license that allows for the access, usage, modification, and distribution of the provided entity, and whose information on usage is made publicly available."

While open-source AI models are exempt from the transparency obligations under Article 53(1), the current framework offers only limited regulatory consequences for open-source AI systems under Article 2(12), as only Article 4 does not apply to them.

### ii. The open-source GPAI exemption problem

Open-source models are exempt from the transparency obligations in Article 53(1)(a) and (b), unless they qualify as systemic-risk models, under Article 53(2). This exemption raises two distinct concerns. First, the open-source definition does not require disclosure of energy consumption during model training, whereas non-open-source providers must supply such information under Article 53(1) and Annex XI. Second, downstream providers operating in high-risk sectors depend on the transparency elements listed in Annex XII as essential inputs for compliance. These disclosures underpin technical documentation, risk mitigation strategies, human-oversight protocols, post-market monitoring and audit preparation. Without adequate upstream information, downstream actors cannot meet their statutory obligations.

The Act need not extend the Article 53(2) exemption to larger entities that release open-source models. With respect to energy disclosures, the requirements in Annex XI Section 2 points (d) and (e) could apply to open-source model providers unless they fall within the micro, small, or medium- sized enterprise categories defined in the Commission Recommendation of 6 May 2003 (OJ L 124, 20.5.2003, p. 36). Annex XI requires providers to disclose information about the computational resources used to train the model – such as the number of floating-point operations, training duration and other relevant parameters – as well as known or estimated energy consumption. Point (e) allows providers to rely on estimates derived from computational-resource data when direct measurement of energy use is not feasible.

Large technology firms that release open-source AI models possess data-center-scale infrastructure and already maintain sophisticated sustainability reporting systems. They are therefore well positioned to provide precise energy-use information. Such disclosure promotes environmental responsibility, enables policymakers and researchers to compare environmental externalities across model architectures, and creates incentives for efficiency-oriented model design (Alder et al., 2025; Ebert et al., 2024; Hacker, 2024; Kaack, 2022; Luccioni, 2024). Allowing major firms to circumvent equivalent transparency requirements would leave a significant loophole at a time of rapidly rising AI-related electricity demand (Luccioni et al., 2025). Limiting the Article 53(2) exemption to SMEs would reflect proportionality, since smaller actors face resource constraints that hinder

comprehensive energy measurement. Such a limitation would also support downstream compliance in high-risk contexts and offer regulators and the wider public greater visibility into AI's climate footprint (Alder et al., 2025; Hacker, 2024; Kaack, 2022; Luccioni, 2024).

Furthermore, disclosing the items listed in Annex XII is essential for giving downstream providers the information they need to comply when using open-source models. This is a critical use case for AI adoption in Europe, and greater transparency will strengthen the EU's competitiveness in this area.

### b) Ongoing review of GPAI code of practice

The current GPAI Code of Practice requires regular updates to enhance its effectiveness and adoption. To make this process more agile, the Code could be split into three separate instruments aligned with its existing chapters: transparency, copyright, and safety and security. Such a division would allow each code to evolve at its own pace, which reflects the different maturation rates of regulatory approaches and industry practices in these domains. Transparency requirements may stabilize relatively quickly, whereas safety and security standards will require frequent revision as threat environments and technical capabilities continue to shift.

The Commission might also communicate that adherence to the Code offers tangible business advantages beyond regulatory. GPAI providers routinely supply Know Your Business documentation during due diligence and procurement processes. Compliance with the Code of Practice directly supports the preparation of these materials, which clients increasingly expect when assessing GPAI services. The Code thus serves a dual function: it satisfies regulatory requirements while also streamlining commercial transactions. Providers can leverage their Code compliance as evidence of operational maturity and effective risk management, which potentially accelerates sales cycles and strengthens market competitiveness.

## 5. Value chain regulation

A recurring challenge in AI governance concerns regulation across the value chain – from data curation to modeling, fine-tuning and hosting to deploying and use. Here, we focus on three key aspects: the regulation of fine-tuning, collaboration duties, and a voluntary model repository with evidentiary implications in cases of harm.

### a) The regulation of "fine-tuning" and GPAI modifications (Art. 25(1))

The current AI Act contains a significant regulatory gap regarding modifications of GPAI models (Blum & Rappenglück, 2024; Hacker & Eber, 2025; Hacker & Holweg, 2025; Schwartmann & Zenner, 2025; Wendehorst, 2024). Article 25 addresses only modifications of high-risk AI systems, yet the practice of adapting GPAI models for domain-specific tasks is a core element of contemporary AI deployment (Future of Life Institute, 2022). In practice, organizations almost always adapt existing models rather than build new ones from the ground up, which makes the omission particularly consequential.

What is needed, in effect, is an "Article 25 for GPAI" to provide legal certainty for organizations that deploy and customize these models. Such a provision would clarify that minor adaptations do not automatically convert deployers into providers subject to the full suite of obligations under Articles 51-56. The Commission's Guidelines on the scope of the obligations for general-purpose AI models represent an attempt to fill this gap (European Commission, 2025a), but guidelines lack binding force before courts and therefore cannot always supply the level of legal certainty required for operational or investment decisions.

Two primary scenarios could trigger provider status for GPAI model deployers. First, mirroring Article 25(1)(a), any entity that places its own name or trademark on an existing GPAI model could be treated as a new provider (Wendehorst, 2024, para. 76).

This approach recognizes that such branding leverages corporate goodwill toward affected persons and downstream users, thereby justifying full regulatory accountability. Second, consistent with Article 25(1)(b), substantial modification of a GPAI model could create provider status. This principle aligns with established product safety law. The guidelines' FLOP threshold provides a useful indicator: modifications consuming one-third or more of the FLOPs used to train the original model generally constitute substantial modification (European Commission, 2025a; see also Pacchiardi et al., 2025). Below this threshold, deployers could be required to conduct consequence scanning to determine whether the modification materially worsens the model's risk profile – for example, if fine-tuning introduces biased datasets (Hacker & Holweg, 2025).

## b) Value chain collaboration duties (Art. 25(2))

When entities fine-tune or otherwise modify GPAI models, compliance becomes federated, i.e., responsibilities become distributed across the value chain. Different entities need to provide information. Collaboration is therefore essential and should be legally enforceable.

### i. GPAI model providers in the value chain

The evolution of Article 25(2) during the legislative process reveals a loophole in the final AI Act. The European Parliament initially proposed extending collaboration duties to GPAI model providers when their models were directly integrated into high-risk AI systems (Art. 28(2)(2) AI Act in the Parliament's version). This extension, however, disappeared once the foundation model provisions were absorbed into the general-purpose AI model rules in Articles 51–56 (Gössl, 2024, para. 29) – and no equivalent to Article 25(2) was introduced in that new section.

The current Article 25(2) imposes collaboration duties only on providers who initially placed an AI system on the market. When Article 25(1) circumstances arise – such as substantial modification or rebranding – the original provider must "closely cooperate with new providers and shall make available the necessary information and provide the reasonably expected technical access and other assistance." This creates not only the required access rights for downstream providers but also a meaningful enforcement mechanism, as any breach constitutes a violation of the AI Act itself, subject to investigations by the AI Office (but cf. Bosman, 2024, para. 124: no financial sanctions against violation of Art. 25(2), see Art. 99(4) AI Act).

The exclusion of GPAI model providers from Article 25(2) creates a significant regulatory gap. GPAI model providers do not place AI systems on the market; they release models that others incorporate into downstream systems. As a result, when an SME integrates a GPAI model into a high-risk AI system and thereby becomes the system's provider, it cannot invoke Article 25(2) to compel cooperation from the original GPAI model provider. This may leave the SME without essential information required to demonstrate compliance with Article 16's obligations for high-risk systems, which the GPAI model provider may be reluctant to share.

This issue was repeatedly raised in the interviews, as discussed above. Industry participants emphasized that, particularly when open-source AI models are used for fine-tuning or integrated into high-risk settings, deployers and downstream providers often lack any effective legal mechanism to obtain the information needed for compliance.

Article 25(4) partially addresses this gap, but ultimately falls short. It requires providers of high-risk AI systems and third parties supplying components to "by written agreement, specify the necessary information, capabilities, technical access and other assistance." GPAI model providers fall within the category of such third parties, as the second sentence of Article 25(4) clearly shows. However, this provision requires only that an agreement be concluded, not substantive cooperation. Any breach of the collaboration obligation becomes a purely contractual dispute

rather than an enforceable AI Act violation. Under Article 99(4), the AI Office or national authorities may sanction only the failure to conclude an agreement, not the failure to provide substantive cooperation or accurate information (see Bosman, 2024, para. 124; Gössl, 2024, para. 56).

This regulatory gap places European SMEs at a particular disadvantage when they seek to innovate with GPAI models. Open-source GPAI models, which represent crucial innovation infrastructure for smaller companies, explicitly fall under Article 25(4)'s contracting requirement. Yet GPAI model providers, especially large technology firms, typically hold substantial bargaining power in these negotiations. They may decline to supply the technical documentation needed for compliance, impose restrictive contractual terms or simply refuse to contract with smaller entities.

The current framework forces SMEs into an untenable position: they bear full regulatory responsibility as providers of high-risk AI systems, but lack any meaningful mechanism to compel upstream cooperation. Resorting to private litigation against GPAI providers – often in foreign jurisdictions – is an unrealistic option for resource-constrained companies. This asymmetry undermines the AI Act's stated aim of supporting responsible innovation across the European ecosystem.

To close this gap, GPAI model providers could be brought within the scope of Article 25(2)'s collaboration framework whenever their models are integrated into high-risk systems, unless they explicitly prohibit such uses (as already foreseen in Art. 25(2)). This would create a publicly enforceable obligation of substantive cooperation, subject to AI Office oversight and sanctions. To this end, Article 99(4) could also be updated to include Article 25(2)-(4) as sanctionable duties. The amendment could specify that GPAI model providers must supply:

- Technical documentation sufficient for assessing compliance with Article 10 (data governance) and Article 15 (accuracy and performance) requirements
- Information on training data characteristics relevant for bias assessment
- Known limitations and failure modes that could affect high-risk applications
- Reasonable technical access for testing and validation purposes

### ii. Input-output testing up the chain

Furthermore, the collaboration duties in Article 25(2) require clarification through a new recital when provider status changes occur. This recital could specify that downstream entities that become new providers hold a right, under Article 25(2), to test defined input–output pairs on the original GPAI model. Such testing allows them to assess whether harmful outputs stem from their own modifications or whether the underlying model already exhibited problematic behavior. This right is essential for enabling downstream companies to demonstrate non-liability when modified models cause harm.

Clarifying this point would serve an important policy objective: it would support the uptake and customization of GPAI models by European SMEs. When adverse outcomes occur, SMEs could seek to show that the underlying model – not their modifications – produced the damage. This approach helps preserve innovation incentives while promoting a fair and workable allocation of responsibility across the AI value chain.

## c) Voluntary GPAI model reference repository

In our view, the need for clear liability attribution in GPAI deployment necessitates the establishment of a comprehensive model repository system. Although Article 71 of the AI Act establishes registries for high-risk AI systems – limited to metadata – this framework could be expanded to include voluntary repositories for GPAI reference models (Hacker & Holweg, 2025). This expansion would enable providers to de-

posit baseline versions of their models, creating an authoritative reference point for later comparison. The repository would serve a critical function in liability disputes by allowing direct comparison between original and modified models to determine whether harmful behavior originated in the base model or resulted from subsequent modifications.

The repository system could be voluntary but include strong incentives for compliance. When GPAI model providers fail to register original reference models, courts could apply a rebuttable presumption of defect and fault against the original model provider in civil liability cases where harm is caused by a modified GPAI model. If the model is in the repository, the customizing entity can readily check whether the same harm would have occurred in the original model. If it is not in the repository, that defense is unavailable to the customizing entity. In that situation, the presumption would be triggered, effectively forcing the original GPAI model provider to supply the necessary information by exonerating itself (a penalty default, see Ayres & Gertner, 1989). Rebutting this presumption would not require full model disclosure. Providers could offer alternative evidence through verified documentation or demonstrations to neutral third parties under confidentiality agreements, preserving legitimate trade secrets.

A parallel voluntary registry for modified GPAI models would complement the reference repository. Organizations that adapt GPAI models could document key characteristics of their modifications, improving supply chain transparency and enabling the sharing of safety information. Participation would signal a commitment to responsible development and support industrywide learning on modification risks and best practices. Together, these registries would create an accountability infrastructure that balances transparency requirements with intellectual property protection, which advances both innovation and safety across the GPAI ecosystem.

## 6. General obligations

We now examine the research exemptions and AI literacy requirements.

### a) Research exemptions

A central issue with the EU AI Act's research exemptions is the narrow construction of Article 2(6) and (8) (Finck, 2025). Article 2(6), the main exception for non–product-oriented scientific research, limits the exemption to AI systems developed and put into service solely for scientific purposes. This rigidity creates a "publishing paradox." Although openly sharing research artifacts – such as code or models – on platforms like GitHub or Hugging Face is a core practice in modern AI research, and is encouraged by leading AI conferences including NeurIPS, such publication may be interpreted as "making the model or system available on the market" under Article 3(10), even when the publication is noncommercial and intended strictly for research (Wernick and Meding, 2025; Finck, 2025). As a result, there is legal uncertainty about the scope of the research exemptions when it comes to the essential practice of making models available to the research community. We therefore suggest clarifying the application of the scientific research exemption in Article 2(6) to explicitly cover the publication of an AI model or system for purely research purposes (cf. also Finck, 2025).

### b) AI literacy (Art. 4)

Article 4 requires providers and deployers of AI systems to ensure a "sufficient level of AI literacy" among their staff and other individuals involved in operating or using AI systems on their behalf. The term "AI literacy" is defined in Article 3(56).

This obligation applies to all systems covered by the AI Act. Its purpose is to help companies meet the Act's requirements by relying on knowledgeable employees and service providers, and to ensure adequate technical competence in the development and use of re-

sponsible AI systems (Kaufmann, 2025, para. 2). In particular, the requirement is intended to promote a high level of protection for health, safety and fundamental rights. Article 4 has applied since Feb. 2, 2025.

While the general objective is sound, the legislative execution raises concerns. These stem from the provision's vague formulation, it´s unclear relationship to product liability regimes and questions about the proportionality of Article 4.

### i. Uncertainty of requirements

The standard set out in Article 4, originally envisioned as a comprehensive obligation, was diluted during the legislative process (Silva et al., 2025). As a result, there is considerable uncertainty about what the provision requires – an issue that is problematic for several reasons.

Industry interviews confirm this. One provider reported significant uncertainty about what AI literacy is actually supposed to entail. Another provider noted that many customers remain unaware of the obligation despite its already being in force: "It's been active since March, and I'm still amazed that so many people haven't done anything about it yet and that it's still not really considered mandatory."

#### Personal scope of application

The personal scope of application is unclear in several respects. While Article 4 initially addresses providers and deployers, it remains unclear what is meant by the phrase "staff and other persons dealing with the operation and use of AI systems on their behalf." The German wording suggests a contractual relationship in which AI is used, whereas the English version could imply a broader interpretation (e.g., Möller-Klapperich, 2025). For providers and deployers, this creates uncertainty about which individuals fall under their compliance obligations.

The greatest uncertainty likely stems from the question of whether providers and deployers must also ensure AI literacy among affected persons (e.g., Kaufmann, 2025, para. 25). Although affected persons are not mentioned in the text of Article 4, both Article 3(56) and Recital 20 refer to data subjects. If Article 4 were interpreted as extending to affected persons, providers and deployers would have to equip them with sufficient AI literacy to make informed decisions about a given AI system and to understand how the system's use may affect them. At first glance, this interpretation would entail significant additional costs – amounting to broad public education – particularly for SMEs.

#### Legal nature

Some commentators have argued, based on the article's open wording, that the obligations in Article 4 amount merely to an appeal (see Rappenglück/Vonthien, 2025). Although the Commission has since clarified that Article 4 does impose a concrete obligation to act (European Commission, 2025), current scholarship shows that those subject to the rule remain uncertain because of its vagueness. This uncertainty risks turning the obligation into a box-ticking exercise, calling into question its usefulness for achieving the provision's stated objective.

#### Scope of obligations

The vague wording of Article 4, which is relative to its field of application, creates practical uncertainty about when a "sufficient level of AI competence" has been achieved (e.g., Schippel, 2025). The AI Act itself provides no guidance on what measures are required to meet this standard. As a result, the obligation is difficult to quantify, and its implementation is marked by uncertainty.

Admittedly, the open wording allows for a factual assessment of individual cases, thus giving SMEs flexibility to tailor compliance to their specific needs (see also European Commission, 2025). The later addition of the phrase "to the best of its ability" further contributes to this flexibility (Knappertsbusch and Rappenglück, 2025). The Commission's "Living Repository of AI Literacy Practices" should also be viewed positively in this context (Commission, 2025).

Nevertheless, uncertainty about the specific scope of the obligation may encourage bloated compliance structures, which are associated with high costs. This places a disproportionate burden on SMEs, which often lack internal capacity and therefore depend on costly external training and certification (Fleck, 2024). At the same time, there is a risk of de facto underregulation: completing external training may become a mere box-ticking exercise, while truly effective programs – those that foster genuine AI competence – may only be feasible for large companies.

### ii. Relationship to product liability regimes

Little attention has been paid to the connection between product liability and ensuring employee competence. Product liability is comprehensively regulated under the PLD regime and national tort law. In companies that operate on a division-of-labor basis, this creates a need for exculpatory measures by company management (for details, see Wagner, 2024, para. 108 et seq.). These measures must serve the general goal of ensuring safety within the organization's sphere of responsibility.[8] As a result, they also encompass ensuring that employees have sufficient competence. In the context of offering and deploying AI systems, this includes guaranteeing a sufficient level of AI literacy.

Once again, the advantages of tort law standards over those in the AI Act should be noted (see Article 26). Accordingly, one might argue that the purpose of Article 4 is already fulfilled by the existing product liability regime.

### iii. Proportionality of the design

A closer examination of Article 4 also reveals shortcomings in terms of proportionality. The provision applies equally to providers and deployers. While the risks posed by AI systems depend in part on how they are used – and therefore should be addressed by both providers and deployers (Fernandes et al., 2024) – requiring AI literacy under Article 4 appears unnecessary for deployers' staff who are involved solely in administrative use of an AI system. An exemption could be justified where a deployer demonstrates that

- the staff member's role is strictly limited to clerical or administrative tasks;
- the staff member has no access to or authority to modify model parameters or outputs that affect individual outcomes;
- appropriate technical and organizational measures are in place and documented.

Such an exception would apply, for example, to employees using AI-based grammar checking software for text production or AI-based scheduling tools. Likewise, consider a supermarket employee who uses automated checkout systems or shelf-management applications. These tasks are strictly ancillary: the employee interacts only with pre-set interfaces, cannot adjust model parameters or thresholds, and has no influence over the system's decision-making logic.

Such an exception would implement the AI Act's risk-based approach, align with Article 6(3), and avoid unnecessary regulatory burdens for deployers, especially SMEs and startups. In these situations, purely administrative staff cannot reasonably affect the outcomes of an AI system. Where a role is strictly clerical and the user cannot alter model parameters, labels, thresholds or the decision context, the causal link to potential harms is missing. Where an administrative user's activity does not materially increase risk, imposing full training obligations appears disproportionate.

Importantly, any exemption must be limited to roles with no capacity to affect (fundamental) rights.

To avoid misuse, a more functional rather than purely formal assessment of the "strictly administrative role" may provide a more appropriate basis for the exemption.

8 BGH, Case VI ZR 408/94, Judgement of January 30, 1996.

Admittedly, the article's open, normative wording ("to the best of their ability," "sufficient level") leaves room for an interpretation that significantly reduces the requirements for administrative employees on the deployer side. However, given the uncertainties outlined above – particularly for SMEs and startups without extensive legal resources – an explicit exemption for strictly administrative staff would be desirable.

This proposal does not deny that everyone should engage meaningfully with AI systems and the risks they pose, especially in the workplace. But a legal obligation does not appear necessary in all contexts.

In our view, this means that supervisory authorities must take action. In their oversight role, they must ensure that the sensible obligation set out in Article 4 can be met entirely with a company's internal resources. To this end, the competence-assurance measures in Article 4 may benefit from being be oriented not only toward mitigating potential risks but also toward promoting "AI enablement."

## 7. Technical standards

The EU's ambition to become a global leader in secure, trustworthy and ethical AI (European Commission, 2022) is to be realized largely through technical standards. The AI Act explicitly assigns technical standardization a central role. Technical standards help operationalize legal requirements and make them more prescriptive (comprehensive Micklitz, 2023; see also Yeung, 2025, Part I).

Article 40(1) provides the normative basis for harmonized standards and the presumption of conformity for high-risk systems (see also Gerdemann, 2024; Kilian and Denga, 2024). Under Article 40(2), the Commission issued a standardization request to the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) in May 2023 (European Commission, 2023). Once published in the OJEU, those standards will form the basis for the presumption of conformity under the Act.

CEN-CENELEC JTC 21 is advancing roughly 35 standardization activities, with over 300 experts from more than 20 Member States involved (see https://jtc21.eu/about/). Despite this substantial effort, the process faces tight timelines, complex stakeholder dynamics, high implementation costs and significant challenges of operationalization (see Kilian, et. al., 2025).

### a) Complexity

The complexity of the standards raises concerns across multiple domains. Challenges arise from the difficulty of defining compliance boundaries when systems combine multiple components or rely on third-party models. Divergent secrecy requirements across Member States further exacerbate operational conflicts in sectors such as legal technology (Kilian et al., 2025). Classification ambiguity compounds these issues for firms operating across sectors.

Reaching agreement on and interpreting the standards is also an arduous task. Competing interests between global and sector-specific standardization needs intensify divergent industry requirements – an issue typical of horizontal standards (Castets-Renard and Besse, 2023). The integration of AI into existing regulatory frameworks adds yet another layer of complexity. Companies report substantial uncertainty about the specific evidence needed to demonstrate compliance, particularly with regard to bias testing and model robustness.

### b) Accessibility

Another core issue concerns the accessibility of the technical standards. In March 2024, the CJEU ruled in the Malamud case that harmonized standards referenced in EU product-safety law as the basis for a presumption of conformity form part of EU law and therefore must be freely accessible and available at no cost.[9] The ruling, however, has met resistance: ISO and IEC filed suit against the European Commission

9 CJEU, Case C-588/21 P ("Public.Resource.Org and Right to Know v Commission and Others").

before the CJEU on Dec. 6, 2024, seeking to protect their copyright in technical standards incorporated into EU harmonized standards.[10]

CEN-CENELEC JTC 21's program includes roughly 35 standards, and acquiring these specifications could cost thousands of euros for each AI provider attempting to determine which requirements apply – given that individual standards typically cost between €100 and €300. The inability to rely on harmonized standards may lead to a negative presumption of conformity and bias by supervisory authorities against alternative compliance routes, such as expert legal opinions (Gerdemann, 2024). Non-compliance carries steep penalties – up to €35 million or 7% of global turnover under Article 99 – and may restrict market access, placing smaller companies at a competitive disadvantage (see Kilian et al., 2025; referring to European Commission, 2021). It is therefore essential to ensure that the standards are openly and freely accessible to all deployers and providers.

### c) Timeline

The timeline for developing the technical standards is highly ambitious and increasingly tight. The Commission initially set an April 2025 deadline, later extending it in June 2025 to Aug. 31, 2025 (European Commission, June 2025). As of this writing (November 2025), the standards have still not been published.

Even once the standards are finalized, the Commission must assess and publish them in the OJEU, a process that can take several months before they become harmonized and trigger the presumption of conformity – an essential step for market access. With final OJEU publication expected no earlier than mid-2026, providers of high-risk AI systems would have, at most, only a few months to comply before the Aug. 2026 application date set in Article 113. This pace raises substantial concerns about practical feasibility (see Kilian, 2025, para. 9).

10 CJEU, Case T-631/24 ("International Electrotechnical Commission and ISO v Commission. Court of Justice of the European Union").

The problem is compounded by the sheer volume of roughly 35 (partially referenced) technical standards under development. Interviewed companies estimate that compliance with a single standard typically requires at least 12 months, even with external support; implementing roughly 35 standards will take far longer. When asked about the most desired amendments, a representative from a large company responded: "Time! More time." Without harmonized standards, costly expert opinions remain the only medium-term route to compliance, a burden that falls disproportionately on smaller firms and risks creating an uneven playing field.

### d) Stakeholder representation

Standardization efforts – now involving more than 1,000 experts across national mirror committees (DIN/DKE, 2024) – face a structural representation problem. Startups and SMEs, which make up 99% of EU companies, lack the resources to participate effectively (StandICT.eu, 2023). The same is true for civil society organizations. Committees are predominantly influenced by large enterprises, often with major U.S. technology and consulting firms forming a participation majority. This disparity disadvantages SMEs, startups, civil-society groups, independent institutions and academia (Kilian, et. al., 2025).

The root cause is resource intensity. Meaningful engagement requires substantial personnel and financial commitments – resources smaller organizations must devote to core operations. As a result, industry associations have become necessary intermediaries to aggregate and represent these stakeholders' interests. But the imbalance gives larger firms competitive and informational advantages, risks skewing standards toward their preferences and raises concerns about adequate representation of EU values – particularly where standards incorporate value-laden trade-offs affecting fundamental rights.

### e) Policy suggestions

In light of the concerns outlined above, the following recommendations are proposed. Given the substantial complexity of the current standards, it is important to limit both the scope and intricacy of technical standards. To ensure that implementation remains feasible, it may be necessary to postpone the application date. Harmonized technical standards are the central compliance tool – especially for smaller organizations – because they allow operationalized legal requirements to be integrated more easily into internal processes, a point repeatedly emphasized in company interviews. In addition, the early publication of near-final drafts would allow companies time to adapt and streamline internal decision-making.

To reflect diverse expertise and avoid systematic disadvantages for smaller European innovators, the standardization process must become more inclusive and better resourced for smaller actors. Policy proposals include lowering formal participation thresholds; establishing substantial EU and national funding programs to subsidize SME and startup participation (explicitly excluding large firms), as well as civil-society input (see also High-Level Forum on European Standardisation, 2024); building EU-level, industry-specific expert networks to provide targeted guidance; and implementing mentorship schemes that pair experienced standardization experts with SME representatives (see https://standict.eu/supporting-smes). Finally, accessibility could be improved through a centralized, free and user-friendly platform and a "standardization guide" system to help newcomers navigate processes and priorities (Kilian, et. al., 2025).

## 8. Article 113 implementation deadlines

Article 113 sets out the provisions on the entry into force and commencement of application of the AI Act.

### a) Postponing the applicability of high-risk requirements

The AI Act's high-risk AI requirements are scheduled to apply beginning Aug. 2, 2026. However, due to the complexity of consensus-building, the development of harmonized standards – one of the cornerstones of effective regulation – is facing significant delays (see above). These standards are a key component of demonstrating conformity (EC 121). Regulated entities must also be able to implement the standards in practice; otherwise, the standards fail to serve their purpose. Under the current timeline, this is not feasible, as substantial delays persist in developing the standards (see p.47. As a result, the industry is calling for a postponement of the date of application of the requirements for high-risk AI systems, for example by 24 months, in order to enable actual implementation (e.g., Bitkom, 2025). Based on the arguments presented above, this demand appears justified. Without such an extension, costly expert opinions remain the only medium-term route to compliance, which disproportionately burdens smaller firms and risks creating an uneven playing field.

One option would be to postpone the application date by 12 months (to Aug. 2, 2027) and delay enforcement of the high-risk rules by an additional 12 months (to Aug. 2, 2028). This would mirror the staggered enforcement timeline for GPAI rules under Article 113, where enforcement follows one year after the application date. Alternatively, national and EU regulators could announce – and the AI Act could codify – a temporary enforcement moratorium for SMEs while the technical standards are still under development and until sufficient implementation time has passed (see Figure 1: Data Structure, category "Extension of Implementation Period").

### b) Transparency obligations

Article 113 also regulates the applicability of Article 50, which imposes transparency obligations on providers and deployers of certain AI systems. While Article 50 covers five different applications and sce-

narios, Article 50(2) is particularly relevant here. It requires providers of AI systems that generate synthetic audio, image, video or text content to ensure that outputs are labeled and recognizable as artificially generated or manipulated (Lauber-Rönsberg, 2025, para. 24). A similar approach can be found in Article 35(1)(k) DSA.

According to Article 113(2), these transparency obligations will begin applying on Aug. 2, 2026. Admittedly, Article 50 as a whole has faced justified criticism, particularly concerning clarity and practical implementation (Bitkom, 2025). Despite this, it is not only sensible to retain the transparency obligations in Article 50(2) – it may even be advisable to move them forward.

The purpose of these obligations is to allow people to distinguish between human-created works and AI-generated content (Martini, para. 62). Given the scale and quality of AI-generated outputs, this differentiation is becoming increasingly difficult. A lack of distinguishability threatens the integrity of the information ecosystem and public trust, creating large-scale risks related to misinformation, manipulation, identity fraud and consumer deception (Rec. 133).

These risks to society as a whole became apparent early on. In March 2022, for example, a synthetic video circulated online showing Ukrainian President Zelensky urging Ukrainians to surrender to Russia. The clip was a deepfake – an AI-generated video produced using deep learning models (BBC, 2022). Since then, complaints about deepfake videos have more than doubled, according to the FBI (CBS News, 2025).

Rapid advances in synthetic content generation – such as Google's Veo 3 (https://gemini.google/overview/ video-generation/) or OpenAI's Sora (https://openai.com/de-DE/sora/) – underscore the urgency of the issue. It is already no longer reliably possible to distinguish human-created works from AI output. A recent Microsoft study from May 2025 confirms this, particularly regarding natural and urban landscape images (Roca et al., 2025).

Given the significant threat to the integrity of the information ecosystem and the emergence of new, largely unforeseeable risks, comprehensive and prompt transparency obligations are of paramount importance. It is therefore proposed that the labeling requirements be brought forward, for example by making them applicable beginning Feb. 2, 2026.

## 9. SME exemptions and support

The AI Act currently provides several exemptions and simplified procedures for SMEs, particularly in relation to conformity assessment procedures and access to regulatory sandboxes.

### a) Size and support

A universal exemption for SMEs – beyond the support measures already in place – may not be warranted under the Act. Civil society organizations interviewed for this study correctly point to a core tension: AI systems developed by SMEs can pose risks to fundamental rights that are identical to those posed by systems developed by large corporations. A poorly designed facial recognition tool or automated hiring system is no less discriminatory simply because its provider employs fewer than 250 people.

Instead of blanket exemptions from substantive requirements, the regulatory framework should maintain consistent standards while offering enhanced support to help SMEs comply. This approach preserves protections for fundamental rights while acknowledging the real resource constraints smaller entities face when navigating complex regulatory requirements.

### b) Proposed support mechanisms

**Regulatory office hours and service desks:** National market surveillance authorities should establish regular consultation sessions where SMEs can receive direct guidance on compliance requirements. These

sessions should be free, confidential and provide actionable feedback on specific AI systems. Importantly, such consultations may also be madeavailable to civil society organizations concerned about AI deployments, helping foster a multi-stakeholder dialogue around responsible development. In Germany, the Federal Network Agency ("Bundesnetzagentur") has offered an AI service desk since July 2025 to perform these tasks (Bundesnetzagentur, 2025). Although not yet formally designated, the agency is expected to become the national market surveillance authority (Referentenentwurf, 2025). At first glance, the service desk appears to meet the requirements described, providing a compliance compass, informational materials, contact channels and free training courses. In addition, the European Commission has launched an AI Act Service Desk (European Commission, 2025). It is essential that comparable services be expanded to all Member States.

**Sector-specific implementation guidelines:** National authorities should develop detailed guidelines that translate high-risk requirements into practical steps for common SME use cases. For example, a guideline for SMEs deploying recruitment AI should specify the exact documentation required, provide templates for risk management frameworks and offer concrete examples of acceptable bias testing procedures. These guidelines should be developed in close consultation with SME associations to ensure practical relevance.

**Technical assistance programs:** The EU could establish technical assistance programs that give SMEs access to:

- Standardized testing tools for bias detection and performance assessment
- Template documentation packages for common AI applications
- Shared conformity assessment resources to reduce individual costs
- Expert networks offering specialized guidance on data governance and risk management

**Financial support instruments:** Direct financial support through existing EU funding mechanisms – such as Horizon Europe and the Digital Europe Programme – could prioritize SME compliance costs. This may include voucher schemes for conformity assessments and AI compliance training, grants for bias auditing tools and subsidized access to legal expertise.

# IV. Conclusion

The study demonstrates that effective simplification of European AI regulation depends on clarity, coordination and sustained institutional support – not deregulation. Stakeholders across sectors express a strong commitment to trustworthy AI but face growing uncertainty due to fragmented rules, overlapping obligations and limited guidance. Simplification should therefore focus on disentangling redundant requirements, aligning sectoral and horizontal frameworks and providing transparent, practical tools for compliance.

A coherent and proportionate AI governance system must preserve the EU's constitutional balance between innovation and rights protection. By refining definitions, strengthening accountability and ensuring consistent enforcement, the Union can support both competitiveness and legitimacy. In this sense, simplification – understood as clarification and disentanglement – becomes a pathway toward a more agile, rights-respecting and future-ready digital regulatory framework for Europe.

Table 2 | **Overview of Proposed Actions**

| Short-term actions | |
|---|---|
| **Proposed Actions** | **Responsible Actor** |
| Explicitly prohibit ex post-remote biometric identification with narrow exceptions parallel to real-time RBI | European co-legislators |
| Remove duplicative credit/insurance items from Annex III or extend Article 17(4) integration | European co-legislators |
| Move Annex I A cases to Annex I B and rely on sectoral updates until Aug 2028 | European co-legislators |
| Expand Article 10(5) to all AI systems and GPAI models and allow use before high-risk obligations take effect | European co-legislators |
| Replace accuracy with appropriate performance in Article 15 | European co-legislators |
| Clarify or delete redundant monitoring duties in Article 26 while retaining information duties | European co-legislators |
| Apply FRIA to all or no private deployers; align terminology with Article 9 | European co-legislators |
| Include GPAI providers in Article 25(2) and add sanctions in Article 99(4) | European co-legislators |
| Create dedicated Article 25 framework for GPAI with 1/3 FLOP threshold to determine provider status | European co-legislators |
| Uniform OS definition in Article 3 | European co-legislators |
| Transparency obligations for non-SME OS model providers to enable downstream compliance, including energy disclosure | European co-legislators |
| Exempt administrative staff from AI literacy rules and clarify personal scope of Article 4 | European co-legislators |
| Free access to standards; subsidies for SME participation; operationalization guidance | European co-legislators; Member States; ESOs |

| | |
|---|---|
| Postpone high-risk rules to Aug 2027 and implementation to Aug 2028, or introduce SME enforcement moratorium | European co-legislators |
| Regulatory office hours, sector-specific implementation guidance, technical assistance and financial support for SMEs and CSOs | European Commission; Member States |
| **Medium-term measures** | |
| **Proposed Actions** | **Responsible Actor** |
| Create separate employment-focused "AI at work" instrument under Article 153 TFEU | European co-legislators |
| Remove employment from Annex III after separate instrument under Article 153 TFEU is initiated | European co-legislators |
| Enhance operationalization of standards through delegated acts and sectoral thresholds | ESOs; European Commission |
| Prioritize capacity-building for enforcement bodies, market surveillance authorities and notified bodies | European Commission; Member States |
| **Long-term reforms** | |
| **Proposed Actions** | **Responsible Actor** |
| Establish long-term SME and CSO support mechanisms with stable finance streams | European Commission; Member States |
| Build robust GPAI enforcement ecosystem across value chain | European Commission; Member States; ESOs |

# References


Alder, N., Ebert, K., Herbrich, R., & Hacker, P. (2025). AI, climate, and transparency: Operationalizing and improving the AI Act. Journal of European Consumer and Market Law, 166–170. arXiv preprint arXiv:2409.07471.

Alvesson, Mats, Hardy, Cynthia, & Harley, Bill (2008). Reflecting on Reflexivity: Reflexive Textual Practices in Organization and Management Theory. Journal of Management Studies, 45(3), 480–501.

Andersen, C. K. (2025). Coded panic: Global techno-authoritarianism and algorithmic surveillance of queer bodies. Dialogues on Digital Society, 29768640251379100.

Atabey A., Urquhart L., Schafer B. (2024). Article 72. In C. N. Pehlivan, N.Forgó & P. Valcke (Ed.), The EU Artificial Intelligence (AI) Act : A Commentary.

Auer, M. (2025). Privatrecht und Grundrechte – Eine Neubetrachtung im Jubiläumsjahr. Archiv für die civilistische Praxis, 225(1), 2–45.

Ayres, I., & Gertner, R. (1989). Filling gaps in incomplete contracts: An economic theory of default rules. Yale LJ, 99, 87.

BBC News (2022). Deepfake presidents used in Russia-Ukraine war. https://www.bbc.com/news/technology-60780142.

Bitkom (2025). AI Act Simplification: For Innovation and Feasibility, https://www.bitkom.org/sites/main/files/2025-06/bitkom-publication-ai-act-simplification.pdf.

Blum, B., & Rappenglück, J. (2024). Fine-Tuning von GPAI-Modellen nach der KI-Verordnung: Eine Regelungslücke für Zukunftstechnologie? Computer und Recht, 40(9), 626–632.

Bosman, S. (2024). Art. 25 KI-VO, in: Schefzig and Kilian (eds.), BeckOK KI-Recht. 3rd Ed. 1.8.2025. Beck.

Bundesnetzagentur (2025). KI-Service Desk. https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/start_ki.html.

Castets-Renard, C., & Besse, A. (2022, August 29). Ex ante accountability of the AI Act: Between certification and standardization, in pursuit of fundamental rights in the country of compliance. SSRN. https://ssrn.com/abstract=4203925.

CBS News (2025). Complaints about deepfake AI videos more than doubled this year, FBI says. Here are warnings from experts. https://www.cbsnews.com/newyork/news/deepfake-artificial-intelligence-videos/.

Colombi Ciacchi, A. (2018). Egenberger and comparative law. European Journal of Comparative Law and Governance, 5(3), 207–211.

Cordes, J., & Hacker, P. (2025). AI and Finance: From the AI Act to Sectoral Regulation. International Journal for Financial Services 2024(4), 23–32.

Denga, M. (2021). Plattformregulierung durch europäische Werte: Zur Bindung von Meinungsplattformen an EU-Grundrechte. Europarecht (EuR), 56(5), 569–596.

Denga, M. (2025). Article 26. In J. Schefzig & R. Kilian (Ed.), Beck'scher Online-Kommentar KI-Recht (BeckOK KI-Recht). C. H. Beck.

Denga, M. (2025). Article 27. In J. Schefzig & R. Kilian (Ed.), Beck'scher Online-Kommentar KI-Recht (BeckOK KI-Recht). C. H. Beck.

DIN/DKE. (2024, July 17). Europäische KI-Normung – Endspurt zum AI Act. https://www.din.de/resource/blob/1118040/21c9ee1e795105d3d552d8e636ac303f/gesamtpraesentation-ki-webinar-data.pdf.

Djeffal C. (2025). Article 72. In J. Schefzig & R. Kilian (Ed.), Beck'scher Online-Kommentar KI-Recht (BeckOK KI-Recht). C. H. Beck.

Djeffal C. (2025). Article 82. In J. Schefzig & R. Kilian (Ed.), Beck'scher Online-Kommentar KI-Recht (BeckOK KI-Recht). C. H. Beck.

Ebert, K., Alder, N., Herbrich, R., & Hacker, P. (2024). AI, climate, and regulation: From data centers to the AI Act. arXiv preprint arXiv:2410.06681.

Europäische Kommission. (2025, April 16). Living repository of AI literacy practices (Version of 16. April 2025). https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy.

Europäische Kommission. (2025, May 7). AI literacy – Questions & answers (Version of 7. Mai 2025). https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers.

European Commission (2025). Shaping Europe's leadership in artificial intelligence with the AI continent action plan. https://commission.europa.eu/topics/eu-competitiveness/ai-continent_en.

European Commission. (2021). Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX.

European Commission. (2022). An EU strategy on standardisation: Setting global standards (COM(2022) 31 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0031.

European Commission. (2023). Commission implementing decision of 22 May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence (C(2023) 3215 final). https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en.

European Commission. (2025). Commission implementing decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards high-risk AI-systems in support of Regulation (EU) 2024/1689 of the European Parliament and of the Council and repealing Implementing Decision C(2023)3215. https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)3871&lang=en.

European Commission. (2025). Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final.

European Commission. (2025). Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5045 final.

European Commission. (2025a). Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5045 final.

Fernandes, J.; Holmes, A., & Zhgentin, B. (2024). Article 4. In M. Pehlivan, K. Forgó, & P. Valcke (Hrsg.), The EU Artificial Intelligence (AI) Act – A Commentary. Nomos.

Finck, M. (2025). In Search of the Lost Research Exemption: Reflections on the AI Act. GRUR International, ikaf100.

Fleck, J. (2024). AI literacy als Rechtsbegriff. Künstliche Intelligenz und Recht (KIR), 2024(3), 99–103.

Fornasier, M. (2015). The impact of EU fundamental rights on private relationships: Direct or indirect effect? European Review of Private Law, 23(1), 29–46.

Freyer, O., Jayabalan, S., Kather, J. N., & Gilbert, S. (2025). Overcoming regulatory barriers to the implementation of AI agents in healthcare. Nature Medicine, https://doi.org/10.1038/s41591-025-03841-1, 1–5.

Future of Life Institute. (2022). General-Purpose AI and the AI Act (White paper). Future of Life Institute.

Gabrielli, G. (2025). The use of facial recognition technologies in the context of peaceful protest: The risk of mass surveillance practices and the implications for the protection of human rights. European Journal of Risk Regulation, 16(2), 514–541. https://doi.org/10.1017/err.2025.26

Gerdemann, T. (2024). Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI. MMR – Multimedia und Recht, 27(MMR-Beilage), 614–620.

Giannini, A., & Tas, S. (2024, December 10). AI Act and the prohibition of real-time biometric identification: Much ado about nothing? Verfassungsblog. https://doi.org/10.59704/a15aa6e58151c853

Gioia, Dennis (2021). A Systematic Methodology for Doing Qualitative Research. The Journal of Applied Behavioral Science, 57(1), 20–29.

Giovannone, M. (2025, May 9). AI Act and machinery regulation: What changes for the safety of work equipment. Global Workplace Law & Policy. Wolters Kluwer. https://legalblogs.wolterskluwer.com/global-workplace-law-and-policy/ai-act-and-machinery-regulation-what-changes-for-the-safety-of-work-equipment/

Gössl, S. (2024). Art. 25. In M. Martini and C. Wendehorst (Eds.), KI-VO: Verordnung über Künstliche Intelligenz: Kommentar. Beck.

Green, M. D. (2001). The unanticipated ripples of comparative negligence: Superseding cause in products liability and beyond. South Carolina Law Review, 53(4), 1103–1156.

Hacker, P. & Holweg M. (2025). The Regulation of Fine-Tuning: Federated Compliance for Modified General-Purpose AI Models. SSRN Working Paper. Abgerufen von https://ssrn.com/abstract=5289125.

Hacker, P. (2021). A legal framework for AI training data--from first principles to the Artificial Intelligence Act. Law, innovation and technology, 13(2), 257-301.

Hacker, P. (2024). Sustainable AI Regulation. Common Market Law Review, 61(2), 345–386.

Hacker, P. (2024). The AI Act between Digital and Sectoral Regulations. Report. Bertelsmann Stiftung.

Hacker, P. (2024, January 23). Comments on the final trilogue version of the AI Act. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=475760.

Hacker, P., & Eber, M. (2025). The future of credit underwriting and insurance under the EU AI Act: Implications for Europe and beyond. Harvard Data Science Review, 7(3).

Hacker, P., & Passoth, J. H. (2020, July). Varieties of AI explanations under the law. From the GDPR to the AIA, and beyond. In International workshop on extending explainable AI beyond deep models and classifiers (pp. 343-373). Cham: Springer International Publishing.

Hacker, P., Kasirzadeh, A., & Edwards, L. (2025). AI, Digital Platforms, and the New Systemic Risk. arXiv preprint arXiv:2509.17878.

Hartmann S. (2024). Article 82. In M. Martini & C. Wendehorst, KI-VO: Verordnung über Künstliche Intelligenz. C. H. Beck.

Hicks, S. A., Strümke, I., Thambawita, V., Hammou, M., Riegler, M. A., Halvorsen, P., & Parasa, S. (2022). On evaluation metrics for medical applications of artificial intelligence. Scientific Reports, 12(1), 5979.

High-Level Forum on European Standardisation. (2024). High-level forum recommendations on increasing funding for standardization activities at international level. https://ec.europa.eu/docsroom/documents/62954.

Hilgendorf, E., & Härtlein, A. (2025). Article 27. In E. Hilgendorf & A. Härtlein (Eds.), Verordnung über künstliche Intelligenz: KI-VO. Nomos.

Jarass, H. D. (2021). Article 51. In H. D. Jarass (Ed.), Charta der Grundrechte der Europäischen Union: Kommentar. C. H. Beck.

Kaack, L. H., Donti, P. L., Strubell, E., Kamiya, G., Creutzig, F., & Rolnick, D. (2022). Aligning artificial intelligence with climate change mitigation. Nature Climate Change, 12(6), 518-527.

Kaminski, M. E., & Malgieri, G. (2024). Impacted Stakeholder Participation in AI and Data Governance. Forthcoming on Yale Journal of Law and Technology (2024-2025), U of Colorado Law Legal Studies Research Paper, (24–23).

Kaufmann, J. (2025). Article 4. In J. Schefzig & R. Kilian (Ed.), Beck'scher Online-Kommentar KI-Recht (BeckOK KI-Recht). C. H. Beck.

Kilian R., Jäck L., Ebel D. (2025, 23 July). European AI Standards – Technical Standardization and Implementation Challenges under the EU AI Act. EJRR. European AI Standards – Technical Standardisation and Implementation Challenges under the EU AI Act | European Journal of Risk Regulation | Cambridge Core.

Kilian, R. (2025). Article 40. In J. Schefzig & R. Kilian (Ed.), Beck'scher Online-Kommentar KI-Recht (BeckOK KI-Recht). C. H. Beck.

Kilian, R., & Denga, M. (2024). Das Testen und Zertifizieren von KI-Systemen. Neue Juristische Wochenschrift (NJW), 77(41), 2945–2950.

Kilian, R., Schefzig, J. (2025). Article 10. In J. Schefzig & R. Kilian (Ed.), Beck'scher Online-Kommentar KI-Recht (BeckOK KI-Recht). C. H. Beck.

Kingreen, T. (2022). Article 51. In C. Calliess & M. Ruffert (Eds.), EU Charter of Fundamental Rights: Commentary. C. H. Beck.

Knappertsbusch, M., & Rappenglück, F. (2025). KI-Kompetenz und verbotene KI-Praktiken als Compliance-Pflichten für Arbeitgeber. Computer und Recht (CR), 2025, 281.

Langenbucher, K. (2020). Responsible AI-based credit scoring–a legal framework. European Business Law Review, 31(4).

Langenbucher, K. (2022). AI credit scoring and evaluation of creditworthiness–a test case for the EU proposal for an AI Act. Report. ECB

Lauber-Rönsberg, A. (2025). Article 50. In J. Schefzig & R. Kilian (Ed.), Beck'scher Online-Kommentar KI-Recht (BeckOK KI-Recht). C. H. Beck.

Linardatos, D. (2025). § 7. In E. Hilgendorf & L. Roth-Isigkeit (Eds.), Die neue Verordnung der EU zur Künstlichen Intelligenz. C. H. Beck.

Lincoln, Yvonna S., & Guba, Egon G. (1985). Establishing Trustworthiness. In Yvonna S. Lincoln & Egon G. Guba, Naturalistic inquiry (pp. 289–332). Sage Publications Ltd.

Lindholm, A., Wahlström, N., Lindsten, F., & Schön, T. B. (2022). Machine learning: a first course for engineers and scientists. Cambridge University Press.

Luccioni, A. S., Strubell, E., & Crawford, K. (2025, June). From efficiency gains to rebound effects: The problem of jevons' paradox in AI's polarized environmental debate. In Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (pp. 76–88).

Luccioni, S., Jernite, Y., & Strubell, E. (2024, June). Power hungry processing: Watts driving the cost of AI deployment?. In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (pp. 85-99).

Mackay. (1920).Ejusdem Generis Principle of Interpretation, 90 Cent. L. J. 285.

Malgieri, G., & Santos, C. (2025). Assessing the (severity of) impacts on fundamental rights. Computer Law & Security Review, 56, 106113.

Mantelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. Computer Law & Security Review, 54, 106020.

Martini M. (2024). Article 50. In M. Martini & C. Wendehorst, KI-VO: Verordnung über Künstliche Intelligenz. C. H. Beck.

Mayrhofer, A. (2024). Produktsicherheit und Produkthaftung – zwei Seiten einer Medaille mit unterschiedlichen Gravuren. Recht der Digitalisierung (RDi), 4 (10), 492–498.

Mazzini, G., & Bagni, F. (2023). Considerations on the regulation of AI systems in the financial sector by the AI Act. Frontiers in Artificial Intelligence, 6, 1277544.

Medical Device Coordination Group. (2020). Regulation (EU) 2017/745: Clinical evidence needed for medical devices previously CE marked under Directives 93/42/EEC or 90/385/EEC. A guide for manufacturers and notified bodies. MDCG 2020-6.

Micklitz, H.-W. (2023). The role of standards in future EU digital policy legislation: A consumer perspective. ANEC & BEUC. https://anec.eu/images/Publications/other-publications/2023/ANEC-DIGITAL-2023-G-138.pdf.

Möller-Klapperich, S. (2025). KI-Kompetenz. Neue Juristische Wochenschrift, 2025(5), 193–198.

Pacchiardi, L., Burden, J., Martínez-Plumed, F., Hernández-Orallo, J. (2025). A Framework to Categorise Modified General-Purpose AI Models as New Models Based on Behavioural Changes, Fernández Llorca, D., Gómez, E. (editors), Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2760/4372557, JRC143257.

Paolini e Silva, M., Tamò-Larrieux, A., & Ammann, O. (2025, January 16). AI literacy under the AI Act: Tracing the evolution of a weakened norm. SSRN. https://ssrn.com/abstract=5099834.

Paolucci, F. (2024). From global standards to local safeguards: The AI Act, biometrics, and fundamental rights. In N. Menéndez González & G. Mobilio (Eds.), Facial recognition technology (forthcoming). SSRN. https://ssrn.com/abstract=4929132

Raposo, V. L. (2023). The use of facial recognition technology by law enforcement in Europe: A non-Orwellian draft proposal. European Journal on Criminal Policy and Research, 29, 515–533. https://doi.org/10.1007/s10610-022-09512-y

Rappenglück, F., & Vonthien, L. (2025). Art. 4 KI-VO operativ umsetzen – Ein Drei-Säulen-Ansatz für KI-Kompetenz, KI-Governance und KI-Compliance im Unternehmen. Recht der Digitalisierung (RDi), 2025(8), 398–405.

Referentenentwurf ( 2025). Referentenentwurf des Bundesministeriums für Digitales und Staatsmodernisierung Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (Gesetz zur Durchführung der KI-Verordnung). https://netzpolitik.org/2025/referentenentwurf-diese-behoerden-sollen-die-ki-verordnung-umsetzen/#Gesetz%20zur%20Markt%C3%BCberwachung%20und%20Innovationsf%C3%B6rderung%20von%20k%C3%BCnstlicher%20Intelligenz.

Roca, T., Cintron Román, A., Torres Vega, J., Duarte, M., Wang, P., White, K., Misra, A., & Lavista Ferrés, J. (2025). How good are humans at detecting AI-generated images? Learnings from an experiment (arXiv:2507.18640). arXiv. https://arxiv.org/pdf/2507.18640.

Rossi, L. S. (2022). Article 20. In C. Calliess & M. Ruffert (Eds.), EU Charter of Fundamental Rights: Commentary. C. H. Beck.

Schippel, T. (2025). Trainingsvorgaben: Wie kann man KI-Kompetenz nach Art. 4 KI-VO vermitteln? Künstliche Intelligenz und Recht (KIR), 2025(3), 119–124.

Schreiber, A., & Bronner, L. (2025). juris PraxisReport IT-Recht, 2025(7), Anm. 2.

Schwartmann, R., & Zenner, K. (2025). GPAI-Anwendungen auf dem Prüfstand: Die Regulierung der KI-VO entlang der Wertschöpfungskette, EuDIR, 3–9.

Seitz, C. (2024). Grundrechtsschutz und Künstliche Intelligenz. Das KI-Gesetz der EU und die KI-Konvention des Europarats. Europäische Zeitschrift für Wirtschaftsrecht (EuZW), 35(18), 836–846.

Smith, M. L. (2013). Search engine liability for autocomplete defamation: Combating the power of suggestion. Illinois Journal of Law, Technology & Policy, 2013(2), 313–336. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2328465.

Spindler, G. (2021). Algorithms, credit scoring, and the new proposals of the EU for an AI Act and on a Consumer Credit Directive. Law and Financial Markets Review, 15(3-4), 239–261.

StandICT.eu. (2023). Support to SMEs – SME mentorship programme. https://standict.eu/supporting-smes.

Strauss, A., & Corbin, J. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. Sage.

Tracol, X. (2025). The use of facial recognition technologies by law enforcement authorities in the US and the EU: Towards a convergence on regulation? Technology and Regulation, 289–315. https://doi.org/10.71265/nga7v921

Van Bekkum, M. (2025). Using sensitive data to de-bias AI systems: Article 10 (5) of the EU AI Act. Computer Law & Security Review, 56, 106115.

Van Bekkum, M., & Zuiderveen Borgesius, F. (2023). Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?. Computer Law & Security Review, 48, 105770.

Wagner, G. (2023). Liability Rules for the Digital Age: – Aiming for the Brussels Effect–. Journal of European Tort Law, 13(3), 191–243.

Wagner, G. (2024). § 823 BGB. In F. Säcker, R. Rixecker, H. Oetker, B. Limperg & C. Schubert (Ed.), Münchener Kommentar zum BGB. Band 7. C. H. Beck.

Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology, 114(2), 246–257. https://doi.org/10.1037/pspa0000098

Warthon, M. (2023). Artificial intelligence and freedom of assembly. In J. Temperman & A. Quintavalla (Eds.), Artificial intelligence and human rights (pp. 91–103). Oxford University Press. https://doi.org/10.1093/law/9780192882486.003.0006

Wendehorst, C. (2024). Art. 3. In M. Martini and C. Wendehorst (Eds.), KI-VO: Verordnung über Künstliche Intelligenz: Kommentar. Beck.

Wernick, A., & Meding, K. (2025). Beware! The AI Act Can Also Apply to Your AI Research Practices. arXiv preprint arXiv:2506.03218.

Yeung, K. (2025). Can risks to fundamental rights arising from AI systems be ‚managed' alongside health and safety risks? Implementing Article 9 of the EU AI Act, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5560783.

**Address | Contact**

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Phone +49 5241 81-0
www.bertelsmann-stiftung.de

Asena Soydaş
Project Manager
Digitalization and the Common Good
Phone +49 5241 81-81247
asena.soydas@bertelsmann-stiftung.de

BertelsmannStiftung