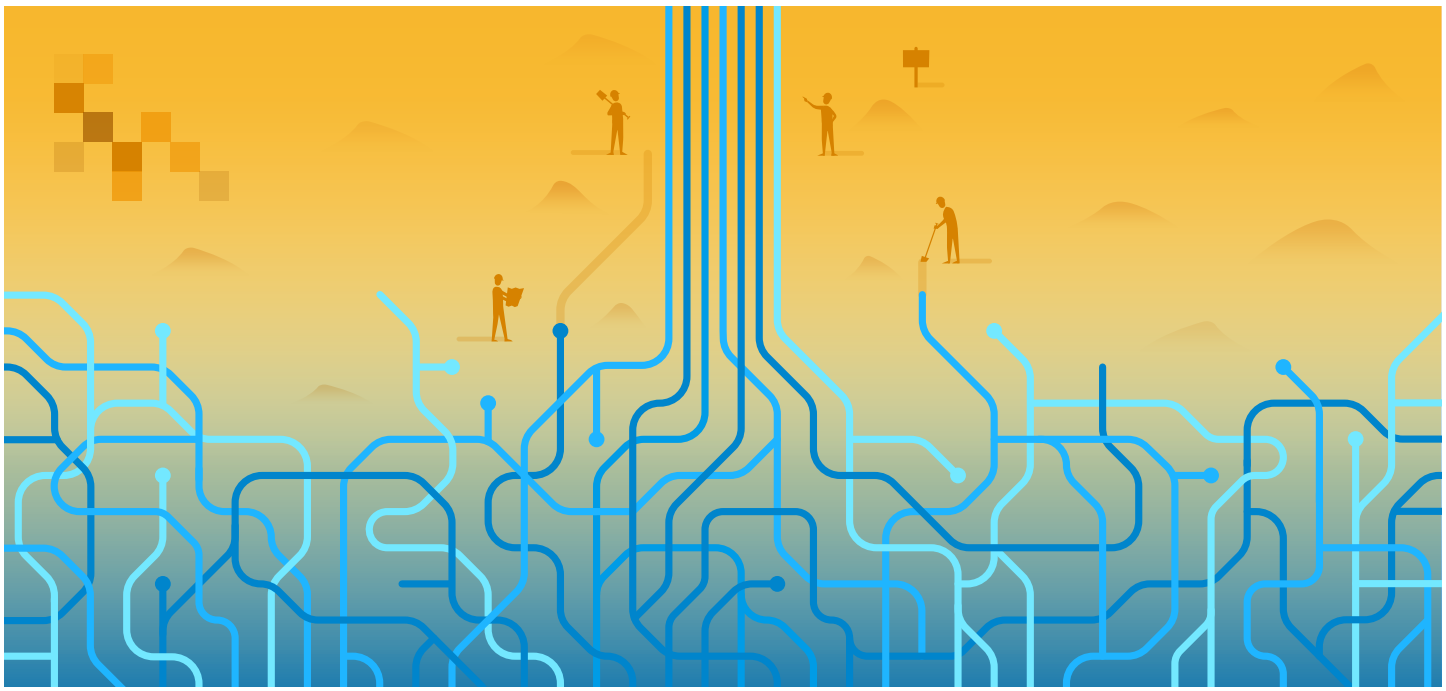

October 2025

# “Simplifying” European AI Regulation:
## An Evidence-based White Paper

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

## Executive Summary

### I. The “Simplification” Challenge

Over the past decade, the EU has emerged as a global leader in digital regulation. The General Data Protection Regulation (GDPR), Digital Services Act (DSA), and Digital Markets Act (DMA) have established comprehensive protections against online harms, anti-competitive behavior, and the uncontrolled use of personal data. The Cyber Resilience Act (CRA) and EU Data Act seek to enhance these protections by promoting a horizontal digital infrastructure and product security architecture. The AI Act continues this tradition. Yet, taken together, Europe’s digital rulebook has created a thicket of interwoven, entangled and partially contradictory acts and rules that is increasingly difficult to navigate. As a result, the policy focus in Brussels has begun to shift from regulation toward competitiveness.

The European Commission has announced a digital omnibus package to be introduced in late 2025 that aims to reduce bureaucratic reporting requirements for companies and harmonize the digital framework. While some civil society organizations (CSOs) warn that the initiative could open Pandora’s box, many in industry view it as an opportunity to incorporate practical implementation experience and align legislation with rapid technological change.

Our empirical research indicates, however, that the AI Act itself is not the main obstacle. Companies struggle most with regulatory fragmentation across overlapping EU instruments. The intersection of the AI Act with the Medical Device Regulation, the Machinery Regulation, and financial services legislation creates particular difficulties. Small and medium enterprises (SMEs) often find it challenging to determine which rules apply to specific use cases and how to demonstrate compliance across multiple regimes. Providers of downstream

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

**Supported by**

GERMAN AI ASSOCIATION

**Commissioned by**

BertelsmannStiftung

high-risk AI systems report additional difficulties accessing relevant compliance information, particularly when working with open-source models, as encouraged by the legislator.

The simplification agenda should therefore balance multiple objectives. The EU seeks to maintain its position as a global leader in secure, trustworthy, and ethical AI while bolstering its competitiveness. Achieving this requires careful calibration: reducing unnecessary regulatory burdens without undermining the fundamental rights protections at the heart of the AI Act. **Our approach emphasizes simplification not as deregulation, but as: 1) clarifying rules and closing loopholes, and 2) untangling overlapping regulations through a more sector-specific approach to prevent double regulation.** Such measures would provide clearer compliance pathways while maintaining robust safeguards in many sectors, simplification will also involve updating provisions on human oversight – a recurring concern across our interviews and analysis.

## II. Empirical Findings

The following section presents findings from interviews and a focus group workshop with key stakeholders on the opportunities, challenges, and implications of the AI Act. Through inductive qualitative analysis, several overarching themes emerged that range from broad support for the Act's objectives to concerns about its practical implementation and suggestions for refinement.

### Methods

The study draws on 15 semi-structured online interviews held in September and October 2025, and a hybrid focus group workshop held in October 2025 with 15 stakeholders. A purposive sampling strategy was employed to capture a broad range of viewpoints on the European AI Act, including those of civil society organizations and private companies of various sizes and sectors (e.g., banking, health care, manufacturing, technology, legal, automotive). Participants operate at the German, European, and global levels. The sample included both deployers and providers of AI systems, including those developing and/or working with general-purpose AI as well as high-risk AI systems.

The interviews lasted between 38 and 55 minutes, with one participant submitting written responses. To structure the discussions and contextualize the data, interview guides and organization-specific dossiers were prepared in advance. With participants' consent, all interviews were recorded, transcribed, and anonymized.

Data analysis was conducted by two researchers using the software MAXQDA, following an inductive approach, well suited to exploring 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 them into second-order categories, and selective coding to develop overarching analytical dimensions.

Analytical quality was ensured through peer briefing, intercoder reliability checks, and member validation. In line with qualitative research standards, reflexivity was maintained through multi-voicing practices to capture diverse perspectives. All interviewees provided informed consent for the inclusion of their quotations, either anonymously or with attribution, in this publication. Selected quotations were translated from German into English.

### Findings

#### Status Quo

Across the interviews, stakeholders express **broadly positive views of the AI Act**, welcoming it as a necessary step toward trustworthy AI governance in Europe. Companies emphasize that a unified European framework helps establish common standards and a level playing field across sectors and member states, while strengthening public trust. The Act is also seen as a way to enhance regulatory clarity while mitigating risks of manipulation, bias, misuse, and abuse.

> *"[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 prob-*

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 Harmonized Digital Regulation 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** | |
| • 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

*lem. 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)*

Amid the current deregulatory shift, civil society organizations continue to defend the AI Act, despite its perceived shortcomings, such as the withdrawal of the AI Liability Directive.

Interviewees also express **critical and ambivalent perspectives**. Many criticisms focus on the legislative process, highlighting procedural inconsistencies and the limited inclusiveness and transparency of consultations. Even so, companies report **actively preparing for the Act** by building internal capacities, governance structures, and workflows. Yet the implementation phase has brought **significant regulatory ambiguities and challenges**, fostering **an atmosphere of fear and uncertainty.** This uncertainty is compounded by perceived time pressures: implementation deadlines are described as "impractical" or "simply not feasible" (Dr.-Ing. Julia Hoxha, CEO Zana Technologies GmbH). Companies worry that regulatory guidelines, often released only shortly before the relevant legal provisions take effect, leave little time for adaptation. Resource constraints further exacerbate these challenges, particularly for smaller firms struggling to absorb the administrative and personnel costs of compliance.

*"[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 criticize the lack of institutional support structures. The absence of clearly defined authorities or points of contact at both the EU and national levels is viewed as a major barrier to effective implementation.

## Substantive Critique

Interviewees also voice broad substantive concerns about the EU AI Act. A central line of criticism centers on **insufficient harmonization across the EU's digital regulatory landscape.** Companies describe how overlapping regimes create simultaneous – and sometimes conflicting – obligations for the same technologies and business areas. This misalignment is attributed to a lack of inter-institutional coordination, with legislative initiatives being developed in parallel and across different Commission directorates.

*"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)*

Companies also point to duplication in reporting, noting that existing frameworks already require much of what the AI Act demands, thereby adding administrative burden without commensurate benefit.

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

Another major source of friction arises from definitional inconsistencies across legal instruments, which can lead to divergent classifications and obligations for identical data or systems, thereby undermining regulatory clarity. For instance, one company reports that differing definitions of "biometric data" (BMW Group) in the AI Act and GDPR result in inconsistent classifications and additional compliance obligations. Similarly, the European DIGITAL SME Alliance described a "compliance dilemma" around fairness testing, caused by conflicting requirements between the AI Act and the GDPR.

*"The restriction on using sensitive data, even for fairness testing, raises practical concerns. Ensuring non-discrimination often requires testing against*

*sensitive attributes to detect bias. […] 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 observe a clear "delta" (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie) between different strands of EU digital regulations, a gap they attribute to the nature of democratic lawmaking. Legislation in the EU emerges through multiple actors, separated powers, and asynchronous timelines, rather than a coordinated, technocratic process.

Another recurring concern involves **overlaps and tensions between horizontal and sector-specific (vertical) regulation.** Companies report that such overlapping obligations lead to unnecessary duplication.

*"[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." (N26)*

Particularly in highly regulated industries such as health care and finance, comprehensive risk management standards are already well established. As Doreen Soeder, Head of Compliance at Tiplu GmbH, notes, the only "really new" element introduced by the AI Act is "human oversight." By adding parallel procedures, the Act increases compliance burdens and dilutes 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 […]." (Dr.-Ing. Julia Hoxha, CEO Zana Technologies GmbH)*

Companies point to capacity constraints among notified bodies, noting that divergent assessment tools and fragmented oversight mechanisms stretch already limited administrative resources even further. For example, under the Medical Device Regulation (MDR), clinical evidence must be provided before obtaining CE marking, whereas the AI Act suggests that CE marking should precede clinical evaluation.

Interviewees broadly recognize the logic of a **risk-based approach** as central to the AI Act, viewing it as a pragmatic and familiar regulatory principle. However, questions remain about whether risks can meaningfully be predetermined through fixed categories without considering the specific context of use. Some describe the broad definition of "high-risk" systems and the related requirements as difficult to implement. The precise delineation of risk categories, they note, remains uncertain.

*"I have lots of questions. Are we prohibited, high-risk or are we low risk? […] There are all these 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)*

CSOs warn that unclear definitions and filtering mechanisms within the Act could lead to loopholes or strategic misclassification, particularly in sensitive areas such as justice.

*"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. […] We said: 'That sounds to us like a loophole to opt out.' […]." (CSO)*

Interviewees widely emphasize that the AI Act leaves critical questions of **accountability along the AI value chain unresolved**. Legal uncertainty persists over how responsibilities are distributed between providers and deployers, particularly in cases involving the fine-tuning of GPAI models. Fine-tuning often occurs without access to necessary technical information, while original model providers tend to distance themselves from liability once modifications are made.

*"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)*

The transitional provisions on fine-tuning under Article 111 are also described as ambiguous – specifically, whether adaptations exceeding the FLOP threshold would constitute the creation of a new model.

Companies further highlight the difficulties of using open-source models in high-risk applications, as they often lack transparency and control over the original 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, companies consistently identify **documentation obligations as burdensome** and, in some cases, redundant, particularly for organizations operating across multiple jurisdictions or within complex corporate structures.

*"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 substantial compliance costs, particularly for SMEs and startups that must allocate resources for compliance from the very start of product development. As one company observes, a start-up "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 smaller companies with limited budgets.

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

## Implications

Companies express concern that the AI Act could inadvertently **slow AI development and adoption across Europe**. To manage regulatory uncertainty and reduce administrative burden, some companies deliberately limit or avoid the use of high-risk AI systems, even at the cost of business opportunities. Several interviewees report growing reluctance among clients to adopt AI-driven solutions, given the tightening regulatory environment. Interviewees also point to lengthier product development cycles due to frequent compliance checks and potential reclassifications. Regulatory hurdles are also seen as contributing to investor hesitation, with some funders perceiving AI-related ventures as overly risky or administratively complex under the new framework.

In response to this uncertainty, interviewees observe a range of **strategic adaptations emerging across the market**. Some organizations have begun referencing compliance in procurement processes, albeit often in vague terms due to the absence of clear standards. At the same time, interviewees observe that companies are adopting divergent implementation strategies.

*"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 […]." (Maria Zerhusen, Head of Research, Empion GmbH)*

Respondents emphasize that the AI Act imposes **uneven regulatory burdens**. SMEs face disproportionate challenges in meeting compliance requirements compared with larger corporations that have dedicated legal teams and greater financial resources. For smaller firms, these constraints risk discouraging AI adoption altogether. This may explain why interviewees note that clients are increasingly turning to large providers, assuming their solutions to be more compliant.

*"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)*

Companies thus warn that such dynamics could consolidating market power among large U.S. corporations, while European SMEs and startups struggle to compete.

Taken together, these trends are seen as potentially hampering innovation in Europe, raising fears that "[t]hat we ultimately end up deterring innovation and effectively stifling this drive to innovate" (Doreen Soeder, Head of Compliance, Tiplu GmbH). Many therefore express concern about the AI Act's potential **impact on Europe's global competitiveness**. They fear a broader erosion of technological sovereignty, as compliance demands divert resources away from innovation and inadvertently deepen Europe's dependency on external technologies and models.

*"Others are moving ahead at tremendous speed, while we'll end up becoming dependent on their AI systems. As a result, our European culture – through the mindsets embedded in their language models – and not only culture but also economic and social ways of thinking will end up being dominated by them." (Carsten Kraus)*

Divergent regulatory frameworks across jurisdictions are seen to further complicate the international deployment of AI systems, making global rollouts both time- and resource-intensive.

As a counterpoint, CSOs challenge the narrative that AI regulation threatens Europe's competitiveness.

*"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)*

## Proposed Actions

A recurring recommendation among company representatives concerns the **timeline** for implementing the AI Act. Current deadlines are seen as unrealistic given the absence of finalized technical standards and guidance documents. Companies therefore call for an extension to allow adequate preparation and consistent compliance across sectors.

*"[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)*

CSOs, however, view such calls critically, warning that extending deadlines could risk reopening the AI Act itself and undermining its implementation. Instead, they advocate for more targeted measures, such as a temporary moratorium for SMEs.

Companies stress that effective implementation of the AI Act depends on **clear, coordinated, and well-supported guidance structures.** Many call for the development of concrete technical standards and predefined compliance elements, to reduce the administrative effort currently required of operators. Technical standards are viewed as essential for translating legal requirements into a language that developers can understand and apply in practice. To address persistent uncertainty around value-chain responsibilities, respondents would welcome templates with clearly defined requirements. Beyond this, several respondents caution against reopening the legislation and instead urge authorities to focus on providing consistent, practical instructions, particularly for interpreting high-risk requirements. Interviewees further recommend establishing central points of contact and unified oversight bodies to prevent fragmented responsibilities across federal, national, and regional authorities.

*"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 […].” (Maria Zerhusen, Head of Research, Empion GmbH)*

SMEs emphasize the need for targeted institutional support, including accessible guidance, funding opportunities, and dedicated points of contact to compensate for their limited compliance capacities. Companies more broadly highlight the importance of **simplifying and better harmonizing the regulatory landscape**, through clearer mapping and coordination between existing and forthcoming regulations.

*“What’s really needed – ideally supported by legislators – is something like administrative guidelines or a data regulation matrix that shows, for example: if you meet requirement X under the AI Act, you also meet requirement Y under the Data Act, and so on. That would be great, especially if it didn’t have to come from lawyers – because that’s expensive.” (SME, legal tech)*

Many companies advocate for closer alignment and cross-regulatory synergies to streamline compliance procedures. Proposals include consolidating documentation into a single, harmonized framework and embedding AI-related standards within existing sectoral regimes. While CSOs acknowledge the need to integrate horizontal and sector-specific (vertical) regulation, they view this as a subsequent step rather than an immediate priority. They caution that simplification should not be equated with deregulation, and that ongoing political debates risk instrumentalizing the AI Act and related EU regulations as bargaining tools in transatlantic negotiations.

*“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)*

Company representatives also advocate for **a more dynamic legislative framework** and stronger involvement of industry actors in regulatory design to help maintain expertise in fast-evolving areas such as generative or agentic AI. CSOs likewise call for greater participation to ensure that the interests of all stakeholders are adequately addressed.

Some interviewees suggest that the AI Act should be **refined rather than reopened or weakened**. They advocate for more nuanced regulation, such as a more differentiated risk taxonomy distinguishing limited from high-risk categories. Yet this idea is contested as “adding more complexity and legal uncertainty” (Michael Kolain, Head of Policy, Zentrum für Digitalrechte und Demokratie). Respondents also call for a clearer delineation of responsibilities along the AI value chain, emphasizing that stronger cooperation between providers and users during deployment and fine-tuning is essential.

CSO representatives, meanwhile, call for stronger safeguards for fundamental rights by closing loopholes, particularly in relation to prohibited real-time biometric identification (RBI).

*“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)*

They also stress the need for uniform transparency obligations, calling for a consistent baseline of disclosure across all actors and for “strong and meaningful fundamental rights impact assessment” (CSO).

# III. Recommendations

Drawing on these empirical insights, we outline the following options for addressing these issues in nine key fields.[1]

## 1. Gaps in Current Regulation

### Post-Remote Biometric Identification

Article 5 prohibits AI practices deemed incompatible with Union values and restricts the use of real-time remote biometric identification (RBI) in public spaces. However, post-remote biometric identification (ex post RBI) is addressed only indirectly, through three non-binding principles set out in Recital 95: proportionality, prohibition of indiscriminate surveillance, and prevention of circumvention. While the GDPR and Law Enforcement Directive (LED) apply and prohibit some ex-post RBI actions (see European Commission, 2025, para. 429), those rules and the Act still leave substantive regulation to the member states.[2] This results in inconsistent protection of fundamental rights across the Union. The temporal distinction between real-time and ex post RBI is unconvincing. Continuous recording followed by delayed biometric analysis can yield the same surveillance outcomes as real-time identification – effectively circumventing Article 5's limits and producing comparable chilling effects on democratic participation, as civil society organizations have warned (see Figure 1: Data Structure, category "Safeguards for Fundamental Rights"). To close this loophole, Article 5 could explicitly prohibit ex post RBI in public spaces for law enforcement purposes, allowing only narrowly defined exceptions that mirror those applicable to real-time RBI. Such an amendment would allow for law enforcement proceedings in severe cases to continue using ex post RBI.

### Value-Chain Collaboration Duties

A further concern for competitiveness arises along the value chain. The current Article 25(2) establishes collaboration duties only for providers who initially placed an AI system on the market. When circumstances outlined in Article 25(1) occur – 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 provision establishes vital access rights for downstream providers and a robust enforcement mechanism, as any breach constitutes a violation of the AI Act itself, which is subject to investigations by the AI Office.

However, GPAI model providers are excluded from Article 25(2), which creates a very significant regulatory gap in one of the most important industry use cases for AI adoption in the EU (cf. Gössl, 2024, para. 29 and 56). When an SME integrates a GPAI model into a high-risk AI system, thus becoming the provider of that system, it cannot rely on Article 25(2) to compel cooperation from the original GPAI model provider. As a result, the SME may lack the essential information needed to demonstrate compliance with Article 16, particularly if the GPAI model provider is unwilling to share relevant data or documentation. Industry participants highlighted this issue in the interviews, especially in connection with open-source AI models used for fine-tuning or integration into high-risk scenarios (see Figure 1: Data Structure, categories "Open-Source Paradox"; "Avoidance of AI or High-Risk Products"; and "Clarification of Responsibilities along the Value Chain"; see also Section II, Substantive Critique)). SMEs reported having no effective legal recourse to obtain the information necessary for compliance. In practice, this makes open-source GPAI models difficult to use in high-risk settings, contradicting the EU's stated goal of fostering broad and inclusive AI adoption.

## 2 | Sectoral Overlap and Redundancy: Toward a More Sectoral Approach

Drawing on interview findings, we identify two potential adjustments that would shift the AI Act toward a more sectoral approach. First, certain elements cur-

1 This section also reflects the authors' own professional judgment and interpretation, which at times may extend beyond or diverge from the empirical findings. The views expressed here do not necessarily reflect those of the interview participants.

2 For example, Art. 10 lit. a LED allows for biometric processing based on any (otherwise constitutional) "Member State law," which opens the door quite widely.

rently listed in Annex III could be removed and integrated into sector-specific regulation – such as a dedicated framework for employment – or incorporated through sectoral updates in areas like credit scoring and insurance. Second, already activities already covered under Annex I could likewise be prioritized. This would imply moving sectors from Annex I A to Annex I B. The distinction would be procedural rather than substantive: laws currently listed under Annex I(A) would no longer intersect directly with the AI Act but would need to be updated by a predetermined date – for example, by August 2, 2028 – to ensure alignment with AI requirements. Based on the interviews and workshop discussions, this adjustment would primarily concern the issue of human oversight. If no AI-relevant update is implemented by August 2, 2028, the "unupdated" sector would revert to Annex I A, thereby maintaining AI-specific coverage.

### Employment Sector

The employment sector offers a compelling case for exclusion from Annex III – not because AI use in the workplace poses no specific and significant risks to affected persons but because it warrants a dedicated legislative framework (see Figure1: Data Structure, theme "Lack of Harmonized Digital Regulation"). Recent hearings in the European Parliament on this matter demonstrates legislative momentum toward this approach.

Such an approach would also better reflect the structure of the EU treaties. For example, the rules on internal market harmonization on which the AI Act's employment sections are based create constitutional barriers to the current framework. This legal basis explicitly excludes "provisions relating to the rights and interests of employed persons" (Article 114(2) TFEU). As a result, specific worker protections in the AI Act (Articles 85-86; Article 26(7) AI Act) may fall outside the Act's legitimate scope, since they extend beyond product regulation in the strictest sense.

A separate directive, adopted under this specific employment legal basis (Article 153 TFEU), would address these constitutional concerns and enable proper consultation with social partners throughout the drafting process, as required under EU social policy procedures (Article 154 TFEU). Such a participatory approach could produce more balanced and effective regulation – one that reflects the unique dynamics of employment relationships and aligns more closely with incumbent and planned employment law initiatives, such as the Platform Work Directive (PWD). Until such a directive is enacted, however, the current rules should remain in force, though.

### Credit Scoring and Insurance

Credit scoring and insurance applications similarly may merit removal from the high-risk category in Annex III, in exchange for sectoral updates until August 2027. Both sectors already operate under comprehensive regulatory frameworks governing algorithmic decision-making and risk management such as Solvency II. The credit scoring regulation and existing financial services regulations create overlapping requirements with the AI Act's provisions. Recent scholarship (Cordes & Hacker, 2025; Hacker, 2024; Hacker & Eber, 2025; Mazzini & Bagni, 2023; see also Spindler, 2021; Langenbucher, 2022) and our interviews (see Figure 1: Data Structure, theme "Tension Horizontal/Vertical Regulation") document how this regulatory duplication imposes unnecessary compliance burdens without corresponding benefits for consumer protection.

The banking and insurance sectors have developed mandatory and sophisticated – though mostly administrative – risk management regimes for AI system validation that often exceed regimes (e.g., in Germany: MaRisk provisions AT 3, AT 4.4, BT 2 versus Article 17). Financial institutions face substantial challenges in determining which horizontal AI Act requirements exceed their current regulatory obligations and therefore demand additional compliance measures beyond established sectoral rules. If kept in Annex III, the financial sector requires integration mechanisms that extend beyond quality management (cf. Art. 17(4) AI Act) to encompass the full set of obligations under the Act. Without comprehensive alignment, credit scoring and insurance applications will continue to face overlapping and potentially conflicting regulatory demands that neither strengthen consumer protection nor promote innovation.

### Medical Devices and Machinery

Health care illustrates similar structural problems with current regulation (see Figure 1: Data Structure, theme "Tension Horizontal/Vertical Regulation"). Medical AI systems are subject to duplicative requirements under both the AI Act and the MDR. The MDR already establishes comprehensive safety and performance requirements for software as a medical device. Layering AI Act obligations on top of this framework introduces additional compliance complexity without demonstrable safety benefits (cf. Yeung, 2025, p. 14-17).

For example, Article 15(1) of the AI Act requires medical AI systems to achieve appropriate "accuracy." However, accuracy is often misguided as a performance metric for medical applications (Hicks et al., 2022). The MDR therefore rightly mandates a sophisticated set of clinical trials and a positive benefit-risk ratio (Article 61, 2(24), and Annex I including Sections 1 and 8 MDR) instead of a blank and misleading accuracy rate. Recent developments in agentic AI systems highlight how rapidly evolving medical AI capabilities demand flexible, sector-specific regulatory responses (Freyer et al., 2025). The MDR's established procedures for clinical evaluation and post-market surveillance provide more appropriate frameworks for addressing these emerging technologies than the AI Act's generic requirements. Issues concerning the timing of CE markings (before or after clinical trials) and the consequences of substantial modifications or changes – including whether further conformity assessment is required – were repeatedly raised in interviews as key points of uncertainty.

Manufacturing presents parallel challenges (see Figure 1: Data Structure, theme "Tension Horizontal/Vertical Regulation"). The overlap between AI Act requirements and the new Machinery Regulation creates particular difficulties for AI-enabled industrial systems (Giovannone, 2025). The Machinery Regulation already addresses the specific risks of industrial AI applications through established conformity assessment procedures. Superimposing AI Act obligations risks complicating this structure: manufacturers must navigate potentially conflicting technical standards and documentation requirements without clear hierarchies or integration mechanisms. As Hacker (2024) notes, a provision analogous to Article 17(4) AI Act – to clarify such relationships – is currently missing.

## 3 | Technical Requirements Reform (Articles 10 and 15)

The AI Act's data governance regime under Article 10 could be restructured to prevent conflicts with existing non-discrimination law while enabling effective bias mitigation (cf. Figure 1: Data Structure, theme "Lack of Harmonized Digital Regulation," and Section II, Substantive Critique). Three reforms could be considered (see also Hacker, 2021; Van Bekkum, 2025). First, Article 10 could recognize the limited applicability of non-discrimination law to mere data curation activities (see Kilian/Schefzig, 2025, para. 15). As demonstrated in CJEU cases Associazione Avvocatura per i diritti LGBTI and Feryn,[3] EU non-discrimination law only extends to preparatory activities under specific conditions: a concrete link to protected activities, decisive influence on outcomes, and sufficient publicity. The mere internal compilation of training data for general-purpose AI systems may fail to meet these criteria. Article 10's current references to bias detection and mitigation create confusion by implying that non-discrimination law governs data curation. This tension forces developers to navigate between Article 10's requirements and non-discrimination law's actual scope.

Second, Article 10(5)'s exception for processing sensitive data should be both materially and temporally expanded (see Section II, Substantive Critique). Currently limited to high-risk systems, this provision ignores that bias detection and mitigation benefit all AI applications. Low-risk systems and GPAI models can still perpetuate harmful biases, and restricting debiasing tools to high-risk applications creates counterproductive incentives to avoid beneficial bias testing for fear of violating Article 9 GDPR (Van Bekkum & Zuiderveen Borgesius, 2023). The specific exception in Article 10(5) should therefore extend to all AI systems and GPAI models where providers can demonstrate a legitimate bias-mitigation purpose. Third, the timing of the (expanded) provision in Article 10(5) actually could apply before the general Article 10 obligations take effect. The current structure creates a temporal paradox:

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

developers may use sensitive data for debiasing only once their systems already required to comply with Article 10 (as of Aug. 2, 2026). This timing renders the exception largely ineffective for its intended purpose of enabling proactive bias prevention during the year leading up to the application of the high-risk rules.

Finally, Article 15's reference to "accuracy" could be replaced with "performance metrics," which is the technically correct term (Lindholm et al., 2022, p. 86 et seqq.; see also Section 2, MDR).

## 4 | High-Risk Deployer Obligations

Article 26 of the AI Act imposes a range of obligations on deployers of high-risk AI systems: they must implement technical and organizational measures, assign qualified human oversight, and meet monitoring, reporting, and documentation duties. From a legal perspective, Article 26(5)'s monitoring obligations appear questionable not because oversight is generally unnecessary, but because such obligations already exist under tort law for any product a deployer uses or controls, including AI systems(Wagner, 2024, para. 890; see Figure 1: Data Structure, category "Redundant Documentation and Reporting Obligations").

Industry interviews reveal significant 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." The provider explained that they proactively address these concerns by explaining what Article 26 means and where they can provide support, yet apprehension remains palpable in the market. A representative of large industrial company managing over 4,000 applications expressed particular concern: "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?"

The Product Liability Directive and national tort law oblige deployers to monitor their systems in agile, context-specific ways. If the deployer also happens to be the manufacturer, the revised PLD applies directly. National tort law, meanwhile, continues to operate in parallel, covering harms not addressed by the PLD. Because tort law is based on general standards, it applies to all AI systems – not only those categorized as high-risk – and therefore may better embody the principle of proportionality. Furthermore, actors can draw on long-established case law, even though national tort laws lack EU-wide harmonization. To the extent that Article 26 duplicates EU and national law, its monitoring duties should be clarified in guidance or reconsidered altogether. By contrast, the specific information duties in Article 26(5)(3-4) provide an adequate warning regime and could remain in place.

### Fundamental Rights Impact Assessment (Article 27)

Article 27 requires certain deployers of high-risk AI systems to carry out a fundamental rights impact assessment (FRIA), including private credit scoring and some insurance deployers. This may provide an opportunity for gathering information on AI deployment. However, the approach also presents concerns since fundamental rights generally bind the state; a direct effect on private entities is an exception regarding specific fundamental rights (Prechal, 2020). Yet, Article 27 mandates that deployers assess impacts on all fundamental rights, a requirement seemingly at odds with Article 51(1) of the Charter of Fundamental Rights (CFR), which limits the Charter's scope primarily to state action.

Imposing this obligation solely on private credit scoring and insurance deployers as the only private entities is difficult to justify under the principle of equality. There are no compelling reasons why banks and insurance companies – rather than other private providers – should be singled out, given that many private-sector high-risk applications also entail risks of discrimination. Accordingly, either all or none of the private entities should fall within the scope of this provision (see Figure 1: Data Structure, category "Safeguardsfor Fundamental Rights").

## 5 | Open-Source and GPAI Models

### Open-Source Definition and Transparency Requirements

The EU AI Act currently lacks definitional consistency for OS AI (cf., e.g., Art. 53(2) vs Art. 2(12)). This creates legal uncertainty. To ensure coherence, the Act should adopt a uniform definition of open-source models and systems in Article 3, which could be based on the definition found in Article 53(2).

Moreover, open-source models are exempt from the transparency rules of Article 53(1)(a) and (b), unless they pose a systemic risk (Article 53(2)). This exemption creates two main problems. First, the open-source definition does not include disclosure of energy consumption for model training, which non-OS providers have to disclose. Second, for downstream providers operating in high-risk domains, the transparency items in Annex XII are not optional – they are foundational. These disclosures enable providers to meet their own obligations under the Act, such as documentation, risk mitigation, human oversight design, post-market monitoring, and audit readiness. Thus, the OS exemption in Art. 53(2) should be limited to SMEs. Non-SME transparency helps downstream providers meet their high-risk obligations and helps regulators and society better understand the climate impact of AI (Alder et al., 225; Hacker, 2024; Kaack, 2022; Luccioni, 2024).

### Fine-tuning and Modifications

The current AI Act contains a significant regulatory gap regarding GPAI model modifications (Hacker & Holeg, 2025; Schwartmann & Zenner, 2025; Wendehorst, 2024). Article 25 addresses only modifications of high-risk AI systems, yet adapting GPAI models for specific tasks represents is now a defining feature of contemporary AI deployment (Pacchiardi et al., 2025). Organizations routinely fine-tune existing models rather than build new ones from scratch, which makes this omission particularly problematic.

The Act would therefore benefit from a dedicated "Article 25 for GPAI" to provide legal certainty – going beyond the European Commission's interpretative Guidelines on GPAI scope (2025a), which may be set aside by courts – for organizations that deploy and customize these models. Such provisions would clarify that minor customizations do not automatically transform deployers into providers subject to the full obligations under Articles 51-56. Two primary scenarios could, however, trigger provider status for GPAI model deployers (Hacker & Holweg, 2025; Wendehorst, 2024).

Rebranding: Similar to Article 25(1)(a), any entity placing its own name or trademark on an existing GPAI model should be deemed a new provider.

Substantial modification: Mirroring Article 25(1)(b), substantial modification of a GPAI model should likewise establish provider status. The Commission's Guidelines' FLOP threshold provides a useful operational criterion: modifications using one-third or more of the FLOPs employed for training the original model generally constitute a substantial modification (Hacker & Holweg, 2025; see also Pacchiardi et al., 2025).

## 6 | AI Literacy

As part of its general obligations, the AI Act requires providers and deployers to ensure a sufficient level of AI literacy. First, the vagueness of this obligation creates uncertainty regarding its scope and personal application. Second, an exemption for deployers' and providers' administrative staff could be incorporated to ensure proportionality.

## 7 | Technical Standards Development

The AI Act explicitly assigns technical standardization a central role in operationalizing legal requirements and establishing a presumption of conformity (Art. 40(1), see Kilian et al. (2025)). The CEN-CENELEC JTC 21 committee is currently pursuing roughly 35 standardization activities. Companies report substantial uncertainty over the specific evidence needed to demonstrate compliance. The timeline for developing the standards is extremely ambitious and the shortened timeline means that implementing all standards is practically impossible, in particular for SMEs (Kilian, 2025). With publication in the Official Journal of the European Union (OJEU) expected no earlier than Q1/Q2 2026, providers of high-risk AI systems would have only six months to meet compliance requirements be-

fore the Act applies in August 2026 – a pace that raises substantial concerns about practical feasibility. Interviewed companies estimate that full implementation of some standards would require at least twelve months. For ca. (partially referenced) 35 standards, implementation will take far longer. Without harmonized standards, costly expert opinions remain the only medium-term route to compliance, which disproportionately burdens smaller firms (see Figure 1: Data Structure, category "Disproportionate Burden on SMEs"; for the current status of the standards, see Kilian, 2025).

Standardization efforts also face a structural representation imbalance. Startups and SMEs lack the resources to participate effectively. Committees are predominantly influenced by large enterprises, creating a disparity that disadvantages SMEs, startups, civil society organizations, independent institutions, and academia.

### 8 | Implementation Timeline Adjustments

The AI Act's high-risk AI requirements are scheduled to apply from August 2, 2026. Given the delays in standard setting, the application date could be postponed by 12 months (August 2, 2027), and the enforcement of high-risk rules by another 12 months (August 2, 2028). This would align the rollout with the staggered enforcement of the GPAI rules under Article 113, where enforcement begins one year after application date. Alternatively – or additionally – national and EU regulators may wish to explore whether an enforcement moratorium for SMEs would be appropriate while technical standards remain under development and sufficient implementation time is lacking (see Figure 1: Data Structure, category "Extension of Implementation Period").

### 9 | SME Support Mechanisms

To ensure fair and effective implementation of the AI Act, SMEs require targeted institutional support. Three types of measures could substantially reduce their compliance burden while fostering innovation and accountability. First, national authorities could issue sector-specific guidelines that translate high-risk AI requirements into practical steps for SMEs. These could include documentation templates, risk management frameworks, and examples of bias testing. More specifically, both the AI Office and national authorities could issue event-driven circular letters, modeled on a newsletter, to provide administratively binding guidance (cf. EU financial regulation). Second, the EU could strengthen SME capacity through technical assistance programs offering standardized testing tools, shared assessment resources, and expert networks. Third, financial measures should help SMEs cover compliance and literacy costs through vouchers, grants, and subsidies, and fund their participation in standardization initiatives.

## IV. Conclusion and Next Steps

The EU AI Act represents groundbreaking legislation that establishes global standards for AI governance. However, implementation challenges threaten its effectiveness. The options proposed in this paper aim to simplify compliance while preserving the Act's central goal: the protection of fundamental rights. These recommendations are grounded in extensive empirical research, including in-depth interviews with AI providers, deployers, and civil society organizations directly involved in applying the Act. A comprehensive final report, expanding on these findings and proposals, will be released in November 2025.

Figure 2 | **Overview of Proposed Actions**

| Area | Article/Section | Current Issues | Proposed Actions |
|---|---|---|---|
| **Prohibitions** | Article 5 | Ex post remote biometric identification largely unregulated – law enforcement can record public spaces and apply biometric identification days later | Explicitly prohibit ex post RBI with narrow exceptions parallel to real-time RBI → simplification as clarification and closing loopholes |
| **High-Risk Classification** | Annex III – Employment | Constitutional issues under Article 114(2) TFEU; conflicts with Platform Work Directive | 1) Create separate directive under Article 153 TFEU<br>2) Then remove from Annex III |
| | Annex III – Credit/Insurance | Duplicative requirements with existing financial services regulations | Remove from Annex III or extend Article 17(4) integration |
| | Annex I A and I B | Annex I A: For example, Medical Device Regulation and Machinery Regulation already provide comprehensive oversight | Move Annex I A cases (mostly) to Annex I B: sectoral updates until Aug 2028 instead of direct AI Act application |
| **Technical Requirements** | Article 10 | Article 10(5) exception currently inapplicable, creates temporal paradox; tensions with non-discrimination law scope | 1) Expand Article 10(5) to all AI systems and GPAI models<br>2) Allow use before high-risk obligations take effect |
| | Article 15 | "Accuracy" requirement misguided – wrong metric for medical, fraud detection, credit scoring | Replace "accuracy" with "appropriate performance" |
| **Deployer Obligations** | Article 26 | Monitoring obligations duplicate existing tort law;<br>creates "insane administrative effort" per interviews | 1) Urgently clarify via guidelines or remove redundant monitoring obligations<br>2) Retain specific information duties |
| | Article 27 | FRIA only for credit/insurance violates equality principle;<br>doctrinal issues with private entities | 1) Apply to all or no private deployers<br>2) Align with Article 9 linguistically ("risk") |
| **Value Chain** | Article 25(2) | GPAI model providers excluded from collaboration duties – SMEs cannot compel cooperation from upstream providers | 1) Include GPAI providers in Article 25(2)<br>2) Add sanctions in Article 99(4) |
| | New Article | No rules for GPAI fine-tuning/modification – unclear when deployers become providers | 1) Create "Article 25 for GPAI"<br>2) use 1/3 FLOP threshold |
| **Open Source (OS)** | Articles 2(12), 53(2) | Inconsistent definitions; even large companies exempt from energy disclosure | 1) Uniform OS definition in Art. 3<br>2) Energy disclosure obligations for OS GPAI providers except for SMEs |
| | Article 2 (12), 53 (2) | Downstream system providers of OS models lack effective legal recourse to obtain necessary compliance information | Implement transparency obligations for non-SME OS model providers to enable high-risk downstream system providers |
| **General Obligations** | Article 4 | Vague AI literacy requirements;<br>unclear scope and personal application | 1) Exempt deployers' and providers' administrative staff<br>2) Clarify scope |
| **Technical Standards** | Article 40 | Standards expensive and still unpublished;<br>implementation period not sufficient;<br>SMEs under-represented | 1) Free access to technical standards<br>2) More subsidies for SME participation in standardization committees<br>3) Push for more operationalization of standards, e.g., sector-specific threshold guidelines |
| **Timeline** | Article 113 | Only ca. 6 months to implement once standards published;<br>synthetic content transparency too late | 1) Postpone high-risk rules to Aug 2027 and enforcement to Aug 2028<br>2) Accelerate applying Article 50(2) to Feb 2026 |
| **SME Support** | Multiple Articles | SMEs face disproportionate compliance burden relative to resources | 1) Sector-Specific Implementation Guidelines<br>2) Technical assistance<br>3) Financial support, incl. vouchers |

Source: own illustration

## 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.

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

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

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.

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.

Hacker, P. & Holweg M. (2025). The Regulation of Fine-Tuning: Federated Compliance for Modified General-Purpose AI Models. SSRN Working Paper. 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., & 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).

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.

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.

Kilian R., Jäck L., Ebel D. (2025). European AI Standards – Technical Standardization and Implementation Challenges under the EU AI Act. European AI Standards – Technical Standardisation and Implementation Challenges under the EU AI Act | European Journal of Risk Regulation | Cambridge University Press, Volume 17.

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.

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

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

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

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).

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.

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.

Prechal, S. (2020). Horizontal direct effect of the Charter of Fundamental Rights of the EU. Revista de Derecho Comunitario Europeo, 66, 407–426.

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

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.

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

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

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.

## Commissioned by


**October 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 |** 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

**DOI 10.11586/2025086**