AI Act Simplification: For Innovation and Feasibility

Bitkom's recommendations for an AI Act simplification package

bitkom

At a glance

AI Act Simplification: For Innovation and Feasibility

Initial position

Significant implementation challenges and unclear requirements threaten the AI Act's goal of mitigating AI-related risks while fostering AI innovation in Europe. To realign the Act with its original intent, the EU Commission has announced an AI Act simplification as part of its competitiveness agenda.

69%

of companies in Germany report that they need help in dealing with the AI Act (Bitkom 2024)

The most important takeaway

As Bitkom, we aim to support the EU Commission's competitiveness agenda by offering key recommendations for a feasibility-focused AI Act simplification package that safeguards innovation:

- **Integrate all high-risk requirements related to Annex I A into sectoral legislation.**

  Annex I should be streamlined by merging its two sections and by extending the more flexible Section B approach — which calls for a carefully controlled adaptation of existing sectoral regulation to the AI Act — to the entire Annex. The AI Act should serve as a maximum harmonisation instrument, ensuring that measures to align sectoral regulation with the AI Act do not exceed its requirements.

- **Postpone the entry into application of high-risk requirements by at least 24 months**

  To ensure high-quality standards and realistic implementation, the AI Act simplification package should extend the timeline for high-risk AI requirements by at least 24 months, as current planning suggests key standards will not be finalized before December 2026 due to the complexity of the consensus-building process.

- **Remove unnecessary provisions**

  The AI Act simplification package must eliminate unnecessary burdens and legal uncertainties created by the AI Act, including common specifications, the registration of AI use cases under Annex III, limited flexibility in post-market monitoring, unjustified access to source code, and additional national requirements.

Content

1 Integrate high-risk requirements related to Annex I A into sectoral legislation

Problem:

Early implementation challenges are exposing the limits of applying horizontal AI rules to established sectoral frameworks, especially for those under Annex I section A. The development of harmonised standards for AI is proving slower and more complex than anticipated. Manufacturers are left uncertain as to how new AI-specific standards will align – or conflict – with existing ones that already govern their products. This uncertainty is bound to create bottlenecks and undermine long-standing compliance pathways.

The problem is particularly acute in the area of conformity assessment. The AI Act introduces obligations that current conformity assessment bodies are neither clearly authorised nor equipped to manage under existing sectoral regimes. In highly regulated sectors such as automotive or medical devices, where notified bodies are already under strain, adding AI-related requirements without a clear integration pathway poses a risk for compounding delays and market disruption.

This regulatory burden will weigh the heaviest on manufacturers in sectors where Europe holds longstanding competitive advantages, such as automotive, machinery or medical equipment.

Risk of double regulation in the automotive sector

Apart from the issues outlined above regarding the sectoral regulations in Annex I, Section A, the automotive sector — covered by Section B — faces a particularly pressing risk of double regulation. Due to the extensive approval requirements set out in Regulation (EU) 2018/858, combined with the diverse technical regulations of the UNECE, all relevant aspects of AI in high-risk applications are already covered in the automotive sector – particularly in the area of autonomous driving and driver assistance systems.

An additional adoption of AI Act provisions into the vehicle type-approval regulation would lead to unnecessarily complex and duplicative documentation obligations,

audits, and risk management systems – without providing any meaningful increase in safety for end users beyond what is already ensured by the existing regulations.

Moreover, such a divergence between EU type-approval regulations and those of the UNECE framework would result in significant additional economic and time burdens for the automotive industry, thereby undermining its competitiveness through new trade barriers.

Solution

For these reasons, Annex I **should be streamlined by merging its two sections and extending the more flexible Section B approach to the entire annex**. This would ensure that AI requirements can be progressively incorporated into sectoral frameworks in a more stable and controlled manner, rather than applying immediately and in parallel with sectoral legislation. Crucially, this would allow harmonised standards for AI to be translated and embedded into sector-specific contexts without undermining existing conformity procedures.[1]

Integration of AI requirements into sectoral frameworks should follow a sequenced process grounded in existing legislation. The goal is not to reopen well-functioning regulatory systems, but to align them with the AI Act in a way that respects their structure and avoids legal uncertainty. For this approach to succeed, the AI Act simplification package must **clarify the AI Act's status as a maximum harmonisation instrument**. Sector-specific measures through delegated acts, implementing acts or technical specifications must not impose requirements beyond the AI Act. This is essential to prevent inconsistent or excessive obligations[2], and would strengthen the replicability of AI harmonised standards, maintaining a unified definition of 'state of the art' across sectors.

Removal of automotive regulations from Annex I Section B

In light of the issues outlined above, we recommend exempting all AI systems covered by the automotive regulations in Annex I, Section B, from the high-risk requirements of the AI Act. Accordingly, the automotive regulations should be removed from Annex I, Section B

[1] This approach is better aligned with Recital 49 AI Act, which calls for sector-specific adaptations 'without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established' under EU product legislation.
[2] Attempts to alter the AI Act's classification logic have already emerged, notably in discussions around the Radio Equipment Directive (Directive 2014/53/EU) and the proposed Toy Safety Regulation (COM(2023) 462 final), such as wrongly classifying AI-based cybersecurity components as safety components and considering that third-party conformity assessments are mandatory even when internal assessments are allowed. It should be clarified that AI systems not constituting a safety component or part thereof in the strict sense fall outside the AI Act's scope. This is essential to prevent sectoral authorities from expanding high-risk obligations to AI systems not intended to be covered, based solely on hypothetical impacts on product performance.

2 Postpone application of high-risk requirements and transparency obligations

2.1 Postpone the entry into application of high-risk requirements by at least 24 months

Problem:

The AI Act's entry into application for high-risk AI requirements is scheduled for August 2026. However, the development of harmonised standards, which are crucial for establishing and demonstrating compliance, is facing significant delays. Officially, the revised standardisation request indicates that standards should be available by August 2025. In practice, however, internal estimates from CEN-CENELEC's JTC21 – the group responsible for drafting these standards – suggest that the first standards may not be ready before mid-2026, and full availability may not be achieved before December 2026.

This timeline raises concerns about the practical feasibility of meeting the AI Act's requirements. Even once standards are published, companies will need adequate time to assess and integrate them into their development and governance processes. Implementing new standards requires adaptation of existing systems, training, and alignment with other internal compliance frameworks.

Solution:

To enable the development of high-quality standards and allow sufficient time for their implementation, the AI Act simplification package should extend the implementation timeline for the high-risk requirements under Annexes I and III by at least 24 months and correspondingly delay the applicability of fines for non-compliance by 24 months in this regard. This extension is justified, as current planning horizons—already considered optimistic given the complex and protracted consensus-building process—indicate that the relevant standards will not be fully finalised before December 2026.

Furthermore, organisations with experience in implementing digital regulations note that compliance with a single standard often requires more than 12 months.[3] Given that the implementation of the AI Act's high-risk requirements is expected to involve around 35 (partially referenced) standards in total, a significantly longer timeframe will be necessary to ensure effective and compliant adoption. Given implementation uncertainties, guidance should ensure parties have appropriate time to cure good faith noncompliance before penalties apply.

This should be coupled with efforts to ensure harmonised rules across EU Member States, aligned with international standards (e.g., OECD, G7 frameworks). Multiple Market Surveillance Authorities (MSAs) across the EU will enforce non-GPAI provisions, creating a significant risk of fragmented interpretations and enforcement across the EU. This risks creating procedural duplication and bureaucratic hurdles. For high-risk AI systems, a transparent mechanism for mutual recognition of interpretations across Member States is necessary.

2.2. Clarify transparency obligations and postpone the entry into application

The transparency requirements under Article 50 lack clarity, potentially leading to different interpretations across regulators, creating unnecessary complexity and also require significant implementation guidance, and such guidance will need sufficient lead time for effective implementation. To ensure a practical and workable approach, the European Commission should take learnings from the GPAI Code of Practice process when starting the work on the Art 50 Code of Practice regarding the detection and labelling of artificially generated or manipulated content, including by providing sufficient time for its negotiation. In view of the importance and technical nature of these technologies, the Commission should postpone the applicability of the transparency requirements, as it remains entirely unclear how they can be implemented at this stage.

3 Remove unnecessary provisions

The AI Act introduces a range of provisions that, whilst aiming to enhance safety and transparency, may instead create unnecessary burdens or legal uncertainties without clear added value. Removing these provisions would maintain the AI Act's core protective goals without imposing impractical obligations

[3] Dr. Kilian et al., European AI Standards, p.26

3.1. Common specifications

The development of harmonised standards plays a crucial role in ensuring that regulatory requirements remain practical, industry-driven and reflective of technological realities. However, Art. 41 allows the Commission to adopt common specifications when harmonised standards are unavailable, delayed or deemed insufficient.

Whilst this aims to address potential gaps, the mere presence of common specifications in the legislative framework discourages investment and engagement in the harmonisation process. **Art. 41 should therefore be deleted.**

The development of harmonised standards within tight timelines already faces challenges, and introducing the option of common specifications creates parallel pathways that do not reflect technological evolution or practical feasibility. It is a shared responsibility between industry and the Commission to ensure that harmonised standards are developed in a timely and inclusive manner. Rather than relying on common specifications as a potential substitute, efforts should focus on strengthening the standardisation process itself.[4]

3.2. Registration of AI use cases under Annex III

Art. 49 mandates that providers register in an EU database their AI systems for use cases listed under Annex III, whether they are high risk or not. Indeed, Art. 6(3) specifies that an AI system, even if listed in Annex III, may still be excluded from high-risk obligations if the intended purpose or context of use do not present a significant risk. In such cases, providers are required to document their internal assessment. However, Art. 49(2) mandates that providers register these non-high-risk AI systems in an EU database.

If a system is determined not to be high risk, subjecting it to registration in the high-risk database creates administrative burden, can cause confusion and may imply obligations that are not applicable. Instead, providers should only be required to document their assessment that the system is not high-risk and be prepared to present this evidence to authorities when requested.

The EU database is in itself concerning for industry and public authorities, as many sensitive AI use cases will be listed there, some publicly accessible, making it vulnerable and creating a wealth of information for malicious actors. Even though some use cases will be restricted from public view, there are no guarantees regarding the security of the information hosted on the database. Additionally, critical infrastructure uses of Annex III(2) will be registered at national level, potentially in each Member State. This

[4] The AI Act already provides flexibility for companies by allowing them to demonstrate compliance through alternative methods if harmonised standards are not available. Whilst this can increase the compliance burden compared to using common specifications, which carry a presumption of conformity, common specifications are not the right solution to this problem. Instead of resorting to measures that undercut the harmonisation process, the focus should be on promptly and realistically addressing the challenges related to the availability and development of harmonised standards. Strengthening the standardisation process itself would ensure that companies can rely on consistent, high-quality standards, reducing the need for ad-hoc solutions.

creates a complex registration patchwork which may be exploited against European and national security interests.

Therefore, the obligation to set up and populate a high-risk and non-high-risk EU database, as well as national databases, **should be removed from the AI Act. Arts 49 and 71 should be deleted accordingly.**

3.3. Post-market monitoring plan

Art. 72(3) requires providers to follow a specific post-market monitoring plan, the framework of which will be designed by the Commission through an implementing act. This approach limits providers' flexibility in developing monitoring plans that are tailored to their specific AI systems and risk contexts.

Additionally, the process for drafting implementing acts allows very limited opportunities for industry consultation and co-design. As a result, companies are unlikely to meaningfully contribute to shaping the framework, raising concerns about its practical feasibility.

To address this, Art. 72(3) should be deleted. Instead, providers should have the freedom to develop post-market monitoring plans that are adaptable to specific operational needs.

3.4. Access to source code

Arts 74(13) and 92(3) grant market surveillance authorities or the Commission the right to access the source code of AI systems in specific situations. This is intended to enhance oversight and ensure compliance when there are indications of non-conformity or safety risks. The practical implementation of this provision, however, raises significant concerns.[5]

Granting authorities access to proprietary source code poses a high risk of data breaches and misuse, particularly because authorities lack the technical means and resources to adequately safeguard the code. In the event of undue access, potential vulnerabilities can be exposed, creating security risks, or the information could be sold or given away to competitors. Such confidential and sensitive information is best handled solely by the providers themselves. Additionally, the requirement to grant source code access may conflict with international trade agreements, such as the EU-Japan Economic Partnership Agreement, which explicitly prohibits forced source code disclosure between the two regions.[6]

Given these security, commercial and legal risks, **Arts 74(13) and 92(3) should be deleted.**

[5] It is important to note that source code in this context refers specifically to the human-readable set of programming instructions and algorithms that determine the functioning, logic and decision-making processes of an AI system or model. It does not include documentation, training datasets, weights, logs or other related elements.
[6] EU-Japan EPA, Chapter 8, Art. 8.73, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan/eu-japan-agreement/eu-japan-agreement-chapter-chapter_en.

3.5. Additional national measures

Art. 82 allows national authorities to require AI providers to take additional measures beyond those specified in the AI Act, 'without undue delay,' if a compliant AI system is deemed to still present a risk.

Whilst the intention is to address emerging safety concerns, allowing individual Member States to impose extra measures creates inconsistent obligations across the EU. If some countries choose to enforce stricter requirements whilst others do not, the single market will suffer; on the other hand, if Member States decide to follow one another's lead, there is a risk of an unchecked expansion of the AI Act's scope. The Commission's proposed oversight is vague and limited, offering little assurance of maintaining consistency across the EU.

Art. 82 should be deleted. Compliance with the AI Act should be sufficient for AI systems to be marketed throughout the EU, without the risk of additional national measures that undermine harmonisation and legal certainty.

4 Readjust and clarify scope

4.1. Clarify open-source exemptions and value chain relationships

Open innovation is a critical factor in fostering Europe's AI ecosystem, with open-source (OS) AI models and components playing a pivotal role. However, the AI Act's current provisions on OS exemptions would benefit from clearer guidance regarding scope, licensing and value chain relationships.

The AI Act simplification package should explicitly acknowledge that mature and widely adopted OS licences – such as Apache 2.0, MIT or GNU GPL – grant users broad freedom to utilise the licensed AI model, system, or component with few or no restrictions on purpose. However, some licences, like RAIL (Responsible AI Licenses), include 'acceptable use' policies to restrict harmful or unethical applications. Without clear guidance, such licences may not benefit from the OS exemption. Moreover, for licences without such safeguards, OS providers might be held responsible if their components are misused in high-risk or prohibited applications.

Furthermore, clarity is needed on whether the open-source exemption of Art. 53(2) continues to apply when an OS GPAI model is integrated as a component within a proprietary GPAI system. This issue becomes particularly complex if the OS model has been retrained prior to integration. In such cases, the exemption should at least remain effective for the OS model components, especially when documentation required

under Art. 53 may not be fully available for these integrated elements. For these reasons, the AI Act simplification package should clarify that:

1. OS licences with responsible use clauses should still qualify for the OS exemption. This would ensure that developers who choose to include ethical safeguards in their licences are not unfairly disadvantaged compared to those who do not.
2. OS components retain their exemption even when they are integrated into proprietary AI systems, particularly if the OS model has been retrained before integration.

4.2. Clarify research exemptions

The AI Act includes a research exemption under Art. 2(6), aimed at excluding AI systems specifically developed and put into service for the sole purpose of scientific R&D from the regulation's scope. However, the current wording may lead to narrow interpretations.[7]

The phrase 'specifically developed' could be interpreted to cover only custom-made AI solutions designed for a particular research purpose, excluding more versatile or GPAI systems used during commercial R&D. Additionally, the term 'sole purpose' may be understood as limiting the exemption to purely academic or non-commercial research, thereby excluding AI systems used to develop commercial products, such as medicines, medical devices or other innovative solutions. This interpretation, which was not the legislators' intent, risks capturing valuable R&D activities that are not intended for direct commercial deployment but are essential for product development and innovation.

To address this risk, the Ai Act simplification should **clarify that under Art. 2(6) 'scientific research and development' encompasses all stages of R&D for any product or service, including those intended for commercial use**, as long as they are not yet placed on the market or put into service.

4.3. Clarify scope of transparency obligations

Article 50(2) of the AI Act requires that «providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated." The provision also allows for exemptions where AI systems serve only an assistive function for standard editing purposes or do not substantially modify the input data or its semantics. However, it remains unclear whether this exemption explicitly covers all forms of purely assistive text transformation, such as summarization or linguistic reformulations. To avoid

[7] Art. 2(6)

ambiguity, **it should be explicitly stated that these forms of assistive text transformation fall within the scope of the exemption.**

4.4. Readjust scope of high-risk AI systems according to annex III 1c (emotion recognition)

The classification of systems as high-risk due to emotion recognition is too broad and should be mitigated through additional exemptions. Clear specification of which attributes are considered sensitive or protected under the EU AI Act is needed. The definition of biometric data as set out in the GDPR could be used.

4.5. Clarify Classifications of Cybersecurity AI systems

Recital 55 of the AI Act explicitly states that components intended solely for cybersecurity purposes should not be classified as safety components. However, it needs to be clarified explicitly that cybersecurity components should not qualify as safety components, even if they are part of radio equipment under the Radio Equipment Directive (Art.6 (1) Annex 1), or part of a machine under the machinery directive (Art.6 (1) Annex 1) or used in critical digital infrastructure (Art.6 (2) Annex 3). AI systems in cybersecurity do not pose but minimize risks for users and should therefore not be classified as high-risk per se but by their actual risks.

5 Update GPAI model regulation in line with technological developments

5.1. Clarify how GPAI rules apply to deployers

The AI Act sets out detailed obligations for GPAI model providers, including additional requirements for models with systemic risk.[8] However, it does not sufficiently clarify how these rules apply to downstream actors who fine-tune or modify GPAI models.

This uncertainty will impact the growth of the AI market in Europe. Companies currently exploring GPAI-based solutions are being deterred from investing or scaling their deployments because they may be drawn into obligations designed for upstream model providers, or even reclassified as providers themselves

To provide legal certainty and proportionality, the AI Act simplification package should **establish that downstream modifiers only become GPAI providers when their modifications are both substantial and result in a new model with general-purpose capabilities**.[9] This would ensure that providers are not unduly captured merely for deploying, fine-tuning or adapting models for domain-specific use cases.[10] Without this anchor, the Commission's upcoming guidelines alone may not be enough to reassure deployers.[11]

5.2. Establish a regular cadence for revising methods to assess the GPAI model and systemic risk thresholds

We also suggest implementing a regular cadence (e.g., annually) for reviewing the GPAI-model and systemic risk thresholds:

- Any compute threshold value is likely to become outdated quickly due to rapid technological progress. We therefore recommend reviewing the concrete threshold

[8] Arts 53 and 55, respectively.
[9] Please also see our more detailed consultation feedback on the GPAI Guidelines, which we have submitted as Bitkom.
[10] These changes could be introduced by refining Recital 97 and adding clarifications to Art. 53.
[11] The forthcoming Commission guidelines are expected to introduce a compute-based threshold to help identify GPAI models. Whilst training compute can be a useful first filter, it is not a durable standalone metric. Model generality, functional breadth and risk context must also be assessed to reflect technological complexity and rapid evolution in the field.

values for the GPAI model at least once a year, and reassessing the thresholds for models associated with systemic risk every six months.

- For systemic risk thresholds in particular: When a capabilities-based approach is eventually adopted (see recommendation 3.2 below), we also recommend introducing a regular cadence to update performance benchmarks that might be saturated.

5.3. Introduce a capabilities-based approach to assessing systemic risk over the long term

As evaluation science matures and reliable benchmarks with lower saturation rates emerge, we recommend either complementing or replacing the compute threshold with a more direct assessment of capabilities associated with systemic risks, such as CBRN weapon development, offensive cyber, and advanced autonomy.

5.4. Provide a grace period for implementing the Code of Practice

The finalization of the GPAI Code is delayed despite the AI Act's intention to have a three-month gap between the Code's adoption (intended to be 2 May 2025) and the start of model requirements (2 August 2025). We recommend providing model providers that sign the Code with a sufficient amount of time, beyond 2 August 2025, to implement the Code's provisions.

6 Establish an Industry Advisory Council for practical business insights

To ensure that the implementation and refinement of the AI Act remain grounded in real-world business practices, the AI Act simplification package should establish an Industry Advisory Council. The Council should hold a formal advisory role towards the independent AI Office, including mandatory consultation processes. This would help guarantee that business insights are systematically integrated into the regulatory governance process.

It is important to clarify that the proposed Council would not duplicate the Advisory Forum set out in Art. 67. The Advisory Forum is designed to include a wide range of stakeholders, including civil society and academia, and is likely to have only limited industry representation. For example, similar bodies, such as the European Data Innovation Board, include just three industry representatives. In contrast, the Industry Advisory Council would ensure comprehensive coverage of the entire AI value chain, allowing all relevant business sectors to participate meaningfully.

7 Allow sandboxes to grant presumption of conformity

Regulatory sandboxes are designed to support testing and compliance efforts by allowing companies to experiment with AI systems in a controlled environment. Established jointly or individually by Member States, these sandboxes will provide a practical space to assess how AI systems meet regulatory requirements.

Currently, Art. 57(7) states that the competent authority will issue written proof of successful sandbox activities. Providers can use this documentation to demonstrate compliance, but it only serves as evidence that may be 'taken positively into account.' This limited recognition fails to reflect the substantial effort involved in successful sandbox participation and does not adequately support companies in demonstrating compliance after exiting the sandbox.

The AI Act simplification package should specify that, **upon successful exit from a sandbox, participating companies receive presumption of conformity** for the tested AI system or model. This would not only enhance the attractiveness of sandboxes but also provide clear benefits to companies willing to actively engage with authorities in the sandbox environment.

8 Resolve AI Act and GDPR friction

8.1. Personal data to improve AI reliability and safety

Problem:

To ensure that AI is reliable and safe, providers often need to process personal data throughout the AI system's development and operational lifecycle. This data is crucial not only during the early stages of development, but also for ongoing monitoring to detect and mitigate issues such as bias and performance degradation. However, the AI Act's current provisions on data processing create unnecessary limitations that may reduce the effectiveness of bias mitigation.

Art. 10(5) of the AI Act establishes an exception to Art. 9 GDPR, allowing the processing of special categories of personal data to detect and correct bias. However, the wording is more restrictive than the GDPR itself, as it requires demonstrating that the processing is 'strictly necessary' rather than simply 'necessary.' This creates a higher burden of proof, potentially discouraging AI providers from engaging in essential data processing that could enhance system reliability and safety. Additionally, Art. 10(5)(e) mandates that special categories of personal data must be deleted once bias has been corrected. This fails to account for the need for continuous bias monitoring throughout the AI system's lifecycle, as bias can emerge dynamically when the system is in use.

Furthermore, the AI Act restricts the re-use of personal data in regulatory sandboxes. Under Art. 59, personal data lawfully collected for other purposes can only be used if the AI system serves a substantial public interest. This narrow criterion excludes companies developing AI systems for other beneficial purposes not explicitly listed, such as cybersecurity, defence, economic resilience, education, food safety and agriculture. This limitation could hinder innovation in fields where AI can deliver significant societal and economic benefits.

Solution:

To address these issues, the AI Act simplification package should:

- Harmonise the standard of necessity between the AI Act and GDPR by replacing 'strictly necessary' with 'necessary' in Art. 10(5);
- Clarify that bias monitoring should continue throughout the AI system's lifecycle and that personal data used for this purpose should not be automatically deleted once initial bias correction has been achieved; and
- Amend Art. 59 to allow companies to re-use personal data they already hold for the testing and improvement of AI systems, under strong privacy safeguards, even if

they do not directly serve a substantial public interest. This would ensure that useful and beneficial AI applications are not arbitrarily excluded from sandbox environments.

8.2. Replace FRIAs with enhanced DPIAs

Problem:

Art. 27 requires providers of high-risk AI systems to conduct fundamental rights impact assessments (FRIAs). These assessments evaluate how the AI system itself may impact individuals' fundamental rights, including human dignity, non-discrimination, and freedoms protected under the EU Charter. At the same time, Art. 35 GDPR requires data protection impact assessments (DPIAs) to assess how the processing of personal data may affect individuals' rights and freedoms.

Whilst the two assessments differ in focus – FRIAs assess the AI system, whilst DPIAs assess personal data processing – in practice they cover overlapping concerns. Conducting both assessments would lead to redundancy and obviously increase the compliance burden for public authorities and companies in scope.[12]

Solution:

Instead of introducing a new assessment, the AI Act simplification package should clarify that the relevant deployers and providers should conduct a DPIA. Art. 27(4) already allows for this possibility, but it needs to be clarified unconditionally to ensure consistency. AI providers should be able to determine whether a DPIA is sufficient for FRIA requirements, reducing duplicate work while upholding comprehensive risk evaluation.

Additionally, the obligation to notify authorities (Art. 27(3)) should be deleted, as DPIAs under the GDPR do not have such a mandatory notification requirement. Similarly, the possibility in Art. 27(5) for the AI Office to develop a separate questionnaire should also be deleted, as it would force companies to align their DPIA practices with an additional template.

[12] Companies may be in scope through public procurement, as private entities providing public services, or as deployers AI systems for selected uses cases covered in Annex III.

9 Harmonize AI Act with other horizontal regulation and sectoral regulations

The AI Act contains numerous inconsistencies and overlaps with horizontal regulation, most notably the GDPR and the Data Act, as well as sectoral regulation. These issues must be addressed urgently to prevent legal uncertainty, redundant reporting obligations, and the risk of overregulation. For a detailed list of friction points and proposed solutions, see the following publication.[13]

[13] This publication will soon be available in English as well.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Janis Hecker | Policy Officer Artificial Intelligence
T +49 30 27576-239 | j.hecker@bitkom.org

Responsible Bitkom Committee
WG Artificial Intelligence

Copyright
Bitkom 2025

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.