DIGITALEUROPE

4 JUNE 2025

Digital simplification package: Our AI recommendations

Setting the global standard for the regulation of artificial intelligence (AI), the AI Act represents a pivotal moment for Europe.[1] As the world's most ambitious and comprehensive AI law worldwide, it has the potential to both lead innovation and ensure safety. However, its complexity and breadth also make it one of the most challenging regulations to get right.

Our recommendations aim to strengthen the AI Act's global success through the upcoming digital simplification package, by addressing some of its most problematic provisions that risk undermining Europe's competitiveness.

Table of contents

[1] Regulation (EU) 2024/1689.

Integrate AI requirements into sectoral laws

- Instead of applying the AI Act directly to products like machinery, medical devices or radio equipment, which are already covered by comprehensive sectoral rules, allow the Commission to introduce AI requirements through these existing frameworks when necessary. This would align all Annex I products with the more flexible approach already used for some of them (Section B).

The AI Act was introduced with the commendable goal of ensuring legal certainty for AI development and use in Europe. It sought to replicate the success of the New Legislative Framework (NLF), which has long provided predictability to manufacturers through harmonised standards and conformity assessments rooted in decades of product safety regulation.

This ambition led to the inclusion of a long list of products already governed by sector-specific NLF legislation in Annex I, alongside other AI systems captured by Annex III and general-purpose AI (GPAI). Annex I categorises products already subject to EU sectoral legislation into two groups:

- Section A, including products such as medical devices, machinery and radio equipment, for which the AI Act's requirements apply immediately in parallel with existing sectoral rules; and
- Section B, covering products like motor vehicles and aircraft, for which the AI Act's obligations will apply only once the Commission updates the relevant sectoral laws – via delegated acts, implementing acts or technical specifications – to integrate AI-specific requirements.

Early implementation challenges are already exposing the limits of applying horizontal AI rules to established sectoral frameworks, particularly those under 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 those 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 medical devices, where notified bodies are already under strain, adding AI-related requirements without a clear integration pathway risks compounding delays and market disruption.[2]

[2] Whilst many AI-enabled medical devices will fall under both the medical device regulations (Regulations (EU) 2017/745 and 2017/746) and the AI Act, not all notified bodies designated under the former intend to seek designation under the latter. According to TEAM-NB, only about 20 out of 44 notified bodies plan to apply. The designation process itself remains unclear and may repeat earlier delays experienced for medical devices. See *Politico*, 'Medtech's AI deep dive,' available at https://pro.politico.eu/news/medtechs-ai-deep-dive.

This regulatory burden will weigh heaviest on manufacturers in sectors where Europe holds longstanding competitive advantage such as machinery or medical equipment. In today's context of geopolitical tension, protectionism and inflationary pressures, adding complexity to product compliance creates a strategic liability. We need an approach that safeguards the competitiveness of Europe's regulated industries.

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.[3]

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 digital 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, nor expand its scope.[4] This is essential to prevent inconsistent or excessive obligations, and would strengthen the replicability of AI harmonised standards, maintaining a unified definition of 'state of the art' across sectors.

Apply only when harmonised standards are available

- Delay the application of high-risk AI requirements until at least 12 months after relevant harmonised standards are published, allowing sufficient time for adaptation.
- Eliminate the adoption of common specifications, which would undermine the successful development of harmonised standards.

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 demonstrating compliance, is facing significant delays. Officially, the revised standardisation request indicates that standards should be available by August 2025.[5] In practice, however, internal estimates from CEN-CENELEC's JTC21 – the group responsible for

[3] 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.

[4] 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.

[5] Draft standardisation request amending implementing decision C(2023)3215 on a standardisation request in support of Union policy on artificial intelligence.

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.

It is important to recognise that the AI Act is the first comprehensive AI law, and that developing harmonised standards for such a broad and complex framework is particularly challenging because existing international standards cannot simply be reused or slightly adapted. The AI Act's requirements reflect European-specific regulatory priorities, necessitating the creation of new standards often from scratch. This complexity justifies a more realistic timeline.

Therefore, the digital package should stipulate an automatic rule that **essential requirements for which harmonised standards are being developed only become applicable 12 months after the relevant standard is published**. This would ensure that companies have sufficient time to prepare and reduce the risk of non-compliance.[6]

Remove common specifications

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 possibility of common specifications discourages investment and engagement in the harmonised standards process.

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.[7] 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 substitute, efforts should focus on strengthening the standardisation process itself.[8]

[6] For example, if a standard becomes available on 2 July 2026, the corresponding requirement should only apply from 2 July 2027. Delaying the entry into application of regulatory requirements is not without precedent. In April 2020, the Medical Devices Regulation (MDR) was postponed by one year – from 26 May 2020 to 26 May 2021 – due to pandemic-related challenges and significant delays in the designation of notified bodies. Since the adoption of the MDR and the In-Vitro Medical Device Regulation (IVDR) in 2017, implementation timelines have been extended multiple times to accommodate practical challenges. Most recently, Regulation (EU) 2023/607 introduced staggered extensions for certain medical devices and in vitro diagnostic devices, addressing ongoing issues with Notified Body capacity and ensuring continuous market availability. Rather than forcing ad-hoc delays, the digital package should already stipulate this backstop mechanism to avoid similar problems.

[7] See DIGITALEUROPE, *Assessing merits and bottlenecks in Europe's standardisation system*, available at https://cdn.digitaleurope.org/uploads/2024/07/DIGITALEUROPE_Assessing-merits-and-bottlenecks-in-Europes-standardisation-system_.pdf.

[8] 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.

The Commission’s **power to adopt common specifications should therefore be deleted**.

Expand the legacy clause

- Exempt AI systems already on the market (including GPAI models) from new compliance obligations unless there are significant changes to their design.

The AI Act includes a legacy clause that exempts AI systems already placed on the market from new compliance obligations, unless their design undergoes significant changes.[9] However, the current formulation may fall short of encompassing all relevant AI systems – in particular GPAI models and their compute-related thresholds, which are expected to be clarified in upcoming Commission guidelines. The digital package should expand the legacy clause to cover all AI systems, including GPAI models, under the same criteria.

Without prejudice to prohibited AI practices, **the legacy clause should also extend to transparency provisions and the rules for GPAI**.[10] This means that AI systems already on the market, including GPAI models, would only come into scope if there are significant changes to their designs or, in the case of GPAI models, if they are modified beyond the compute-based thresholds to become a ‘distinct model’ as opposed to a new ‘model version.’ as per the upcoming guidelines.[11]

Given the rapid pace of AI model development, many models will naturally become gradually in scope due to major updates or new versions being released. However, applying the legacy clause to all AI systems, including GPAI models, would help ensure that existing use cases built on legacy models can continue without being prematurely discontinued. Without this provision, companies may find it more practical to withdraw models from the market rather than comply with new obligations, especially when the cost of compliance outweighs the benefit of maintaining the model.

Remove unnecessary registrations, assessments and oversight

- Abolish the mandatory registration of AI systems, along with the related EU and Member State databases.
- Replace fundamental rights impact assessments (FRIAs) with data protection impact assessments (DPIAs), which are already mandated by the GDPR.
- Delete uniform Commission-issued template for post-market monitoring plans, allowing providers to design plans adapted to their AI systems and risk contexts;

[9] Art. 111 AI Act.

[10] Arts 5 and 50 and Chapter V AI Act, respectively.

[11] The only exception should be the copyright provisions of Art. 53(c)-(d), which should continue to apply from August 2027.

- Protect intellectual property and cybersecurity by ensuring that authorities are not granted access to source code.
- Remove Member States' power to impose unilateral additional obligations, which undermines legal certainty and the single market.

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

Eliminate registration requirements

Art. 49 requires providers to register AI systems listed in Annex III in an EU database, regardless of whether they are ultimately deemed high risk. Yet, not all Annex III systems qualify as high risk in practice, depending on their intended purpose and context of use.[12] Where this is the case, providers must carry out and document an internal risk assessment, but they are still obliged to register the system as if it were high-risk.[13]

This creates confusion and unnecessary administrative burden. Requiring registration in a database specifically created for high-risk AI may give the false impression that such systems are subject to all associated obligations. Instead, providers should only be expected to document their determination that the AI system is not high risk, and be prepared to demonstrate this rationale upon request by the competent authority.

The database itself generates significant security vulnerabilities. It will collect sensitive use cases – some publicly accessible – thus offering an intelligence source for malicious actors. Although limited access provisions exist, no robust guarantees are provided regarding the safeguarding of the data. The problem is compounded by the creation of parallel national databases for critical infrastructure, risking a fragmented patchwork of potentially insecure national systems.[14]

To mitigate these risks, the **obligation to set up and populate a high-risk and non-high-risk EU database, as well as national databases, should be withdrawn**.[15]

Replace FRIAs with DPIAs

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,

[12] Art. 6(3).

[13] Art. 49(2).

[14] Pursuant to Art. 49(5), high-risk AI systems used in the management and operation of critical infrastructure (point 2 of Annex III) must be registered at national level, rather than in the central EU database. This implies that each Member State will need to set up its own national registry, leading to a fragmented registration system across the EU. This inherently conflicts with the need to further harmonise EU cybersecurity legislation, which the digital package also aims to address. See our cyber recommendations, available at https://cdn.digitaleurope.org/uploads/2025/06/Digital-simplification-package-Cyber.pdf.

[15] Arts 49 and 71 should be deleted accordingly.

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.[16]

Whilst the two assessments differ in focus – FRIAs assess the AI system as a whole, 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.[17]

Instead of introducing a new assessment, the digital package should clarify that **the relevant deployers and providers should conduct a DPIA**.[18] Additionally, the **obligation to notify authorities should be deleted** as DPIAs under the GDPR do not have such a mandatory notification requirement.[19] Similarly, **the possibility 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.[20]

Allow tailored post-market monitoring

Art. 72(3) foresees a detailed plan for post-market monitoring to be set 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.

Providers should instead be allowed to design post-market monitoring plans that are adapted to the technical and business context in which their systems operate. The **obligation for a uniform monitoring template should be removed**.

Remove source code access provisions

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.[21]

[16] Regulation (EU) 2016/679.

[17] 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.

[18] Art. 27(4) already allows for this possibility, which needs to be clarified unconditionally to ensure consistency.

[19] Art. 27(3).

[20] Art. 27(5).

[21] 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.

Granting authorities access to proprietary source code poses a high risk of data breaches and misuse. Authorities lack the technical means and resources to adequately safeguard the code – in the event of undue access, vulnerabilities can be exposed, 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 conflicts with international trade agreements, such as the EU-Japan Economic Partnership Agreement, which explicitly prohibits forced source code disclosure between the two regions.[22]

Given these security, commercial and legal risks, **provisions that allow authorities to access source code should be deleted**.

Remove national powers to expand obligations

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.

The power for national authorities to require additional measures should be deleted. Compliance with the AI Act should be sufficient for AI systems to be marketed throughout the EU, without the risk of new national obligations that undermine harmonisation and legal certainty.

Clarify how GPAI rules apply to deployers

- Clarify that deployers are only considered GPAI model providers when substantial modifications result in a new general-purpose model.

The AI Act sets out detailed obligations for GPAI model providers, including additional requirements for models with systemic risk.[23] 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 digital omnibus should **establish that deployers only become GPAI providers when their modifications are both substantial and result in a new model**

[22] 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.

[23] Arts 53 and 55, respectively.

with general-purpose capabilities. This would ensure that providers are not unduly captured merely for deploying, fine-tuning or adapting models for domain-specific use cases.[24] Without this anchor, the Commission's upcoming guidelines alone may not be enough to reassure deployers.[25]

Strengthen AI governance

- Transform the AI Office into an independent body with EU-wide supervisory powers to avoid political influence and ensure consistent implementation.
- Establish an Industry Advisory Council to provide practical business insights.

Establishing a robust and credible governance framework requires ensuring that the AI Office functions as an impartial and authoritative body. Currently, the AI Office is structured as a directorate under the European Commission’s DG CONNECT, lacking institutional independence. This arrangement raises fundamental concerns about separation of powers and impartiality of enforcement.

As it stands, the AI Office not only develops implementing legislation and guidance but also interprets and enforces these rules when conducting investigations and issuing penalties. This dual role creates a potential conflict of interest and undermines the principle of good governance. Moreover, because the AI Office operates within the Commission’s structure, it remains susceptible to political influence, which can compromise objective and consistent enforcement.

To address these concerns, the digital package should stipulate that **the AI Office be restructured as an independent body**.[26] This would enhance the AI Office’s credibility and impartiality by safeguarding its supervisory and enforcement roles from political interference.

Furthermore, the digital package should **grant the independent AI Office expanded EU-level supervisory powers** to ensure the uniform application of the AI Act across Member States. Currently, its supervisory role is primarily limited to Chapter V, which addresses GPAI models. Given the cross-border nature of AI deployment, a more centralised and consistent supervisory approach is essential to reduce the risk of fragmented national practices.

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 digital package should establish an Industry Advisory Council. The Council should hold a **formal advisory role towards the independent AI Office**, including mandatory consultation processes.

[24] These changes could be introduced by refining Recital 97 and adding clarifications to Art. 53.

[25] 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.

[26] This is particularly the case for parts of the AI Safety Unit that will be responsible for performing external evaluations of GPAI models with systemic risk as per Art. 92. This model already exists in non-EU jurisdictions: for instance, the UK’s AI Safety Institute operates separately from regulatory and enforcement bodies.

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.

Empower sandboxes to grant presumption of conformity

- Grant presumption of conformity for AI systems successfully tested in sandboxes, incentivising proactive participation by companies.

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 digital 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.

Protect innovation-friendly practices in AI development

- Ensure the research exemption applies to all R&D phases, including commercial research, as long as the AI system is not yet placed on the market.

- Align rules on using sensitive personal data to fix bias in AI systems with the GDPR’s more flexible interpretation; allow retention of personal data for ongoing bias monitoring; and permit data re-use in sandboxes even outside of narrow public interest cases.

- Confirm that open-source licences with responsible use clauses qualify for the open-source exemption, and that open-source components retain their exemption when integrated into proprietary AI systems.

Clarify the research exemption

The AI Act includes a research exemption, 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.[27]

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, not intended by the legislators, risks capturing valuable R&D activities that precede market entry but are critical to innovation.

To address this risk, the digital package should **clarify that '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.

Leverage personal data to improve reliability and safety

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) 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.[28]

[27] Art. 2(6).

[28] We also note that Annex V(5) requires providers to declare GDPR compliance in the EU declaration of conformity. This declaration, however, is meant to confirm compliance with placement-on-the-market legislation, which the GDPR is not. An AI system cannot itself ensure GDPR compliance, only support it; and providers cannot be held accountable for how deployers handle personal data in practice. We therefore suggest that point 5 of Annex V be deleted.

To address these issues, the digital package should:

- **Harmonise the standard of necessity with GDPR** by replacing ‘strictly necessary’ with ‘necessary’;
- Clarify that **personal data used for bias correction should not be automatically deleted after the initial correction**, recognising that bias monitoring should continue throughout the AI system’s lifecycle; and
- **Allow companies to re-use personal data 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.[29]

Support open-source contributions

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 digital package should explicitly acknowledge that mature and widely adopted OS licences – such as Apache 2.0, MIT or GNU GPL – generally 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.

The digital package should make it clear that 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.

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 digital package should clarify that:

- OS licences with responsible use clauses should still qualify for the OS exemption; and
- OS components retain their exemption even when they are integrated into proprietary AI systems, particularly if the OS model has been retrained before integration.

[29] This complements our recommendations regarding the GDPR in the upcoming digital package. See our data recommendations, available at https://cdn.digitaleurope.org/uploads/2025/06/Digital-simplification-package-Data.pdf.

FOR MORE INFORMATION, PLEASE CONTACT:

Julien Chasserieau

Associate Director for AI & Data Policy

julien.chasserieau@digitaleurope.org / +32 492 27 13 32

Bianca Manelli

Manager for AI & Data Policy

bianca.manelli@digitaleurope.org / +32 499 71 28 89

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.