Brussels, 14th of October 2025

Consultation Statement by the European AI Forum (EAIF) on:

Digital Omnibus (Digital Package on Simplification)

We welcome the opportunity to provide feedback on the European Commission's Digital Omnibus initiative. For European AI startups and SMEs, the current patchwork of digital laws creates disproportionate challenges: overlapping transparency obligations, restrictive data-use provisions, duplicate documentation and assessments, inconsistent enforcement across Member States, and many more. These complexities not only significantly increase costs but also slow down innovation and therefore limit the global competitiveness of European AI companies.

This paper sets out the European AI Forum's analysis of how existing EU legal frameworks burden and hold back European AI companies in key issues such as transparency, data access and reuse, compliance burden, regulatory fragmentation, cybersecurity and open innovation. The position paper provides recommendations for simplification measures across EU regulations to increase innovative strength and competitiveness of European AI companies. Each of the following sections outlines the current regulatory problem, its impact on European AI startups and SMEs, and targeted proposals for the Digital Omnibus to achieve greater consistency, proportionality and legal certainty across the EU.

1. AI Act

Since the AI Act's entry into force in 2024 and with the first provisions becoming applicable, it has become clear that the timeline as well as the implementation in general prove to be quite ambitious and, in several cases, could not be met.

Firstly, it is unlikely that harmonised standards for high-risk requirements will be fully available and operational well before the application date for Annex III systems in August 2026. Even if the standards were made available in the first half of 2026,

providers would have only a couple of months to implement them, which is far too little time for real adoption. Previous studies clearly indicate that implementing these standards would take at least 12 months, making this compliance path infeasible for AI startups and SMEs.

Secondly, applying horizontal AI rules in sectors with already existing legal frameworks (e.g., automotive, medical, machinery, aviation) risks duplicative documentation, strained notified bodies, and divergent technical pathways.

Lastly, the entire AI Act still contains several unclear and vague terminology, which in some cases even conflicts with other EU digital regulations. This therefore creates further uncertainty for AI providers.

Policy Recommendations

- **Adjust the implementation timeline by at least 12 to 24 months.** European AI companies need more time to implement high-risk requirements under Annexes I & III; the application and penalties should therefore be postponed accordingly. Early access to near-final drafts (with change-risk caveats) would enable companies to adapt sooner.
- **Remove or narrow provisions that add burden without safety gain.**
    - **We recommend either removing or at least providing a clear clarification on Art. 4.** This article has caused severe uncertainty regarding its scope and potential paths of compliance among providers and deployers.
    - If an AI system that could classify as a high-risk AI system according to Annex I or III but is exempted from such classification based on Art. 6(3), we believe that it is not necessary to register the AI system in an EU-database, as it is currently required according to Art. 49(2). We therefore recommend **the removal of Art. 49(2)** as well as the phrase *"and AI systems that are not considered as high-risk pursuant to Article 6(3) and which are registered in accordance with Article 6(4) and Article 49"* in Art. 71(1).
- **Presumption of conformity through regulatory sandboxes.** Under Art. 57(7), the relevant authority provides written confirmation upon the successful completion of sandbox activities. Providers can cite this as evidence of compliance, but it is only considered as such. However, we believe that this limited status undervalues the significant investment required and offers little assistance once AI startups exit the sandbox. We therefore recommend amending the current provisions so that a successful exit from the sandbox confers a presumption of conformity on the tested AI system or model. This

would not only be a simplification measure, but would also provide a clear incentive for European AI startups to participate.

- **Streamline horizontal–sectoral interfaces.** We recommend treating the AI Act as a maximum-harmonisation instrument and integrate high-risk obligations for Annex I sectors through their existing frameworks, avoiding duplicated assessments and preserving established conformity routes.

2. AI Act, GDPR and ePrivacy Directive

2.1 Transparency Obligations

The current regulatory framework creates overlapping and conflicting transparency obligations across the AI Act, the GDPR and the ePrivacy Directive. For example, AI providers must label AI-generated content and disclose interactions with AI systems, while simultaneously meeting GDPR information duties and ePrivacy consent prompts. For AI startups, these obligations translate into redundant user disclosures, higher compliance costs and fragmented guidance across Member States. In practice, small teams are forced to engineer multiple parallel transparency mechanisms, from pop-ups to privacy notices, while the technical standards for reliable watermarking remain immature.

This regulatory overlap risks creating confusion for users and disproportionate burdens for innovators. Particularly for early-stage AI companies, maintaining separate systems for user labelling, data-protection information and consent management is highly resource-intensive and disrupts the overall user experience. Startups are therefore forced to dedicate time and budget to overlapping compliance processes that add little practical value to transparency or accountability. Inconsistent guidance among national authorities further increases uncertainty and limits the ability to scale across the EU.

Policy Recommendations

- **Unify transparency obligations across the AI Act, GDPR and ePrivacy.** A single, harmonised disclosure should be sufficient to fulfil all relevant legal requirements, reducing duplication and improving user understanding.
- **Adopt a risk-based approach to AI output labelling.** Mandatory labelling should be limited to high-risk or potentially misleading outputs, while obvious or low-impact AI functionalities should remain exempt.
- **Introduce a technical feasibility clause for SMEs.** Providers applying best-effort watermarking or detection measures consistent with available

standards should be considered compliant until interoperable EU standards are established.

- **Clarify the interaction with ePrivacy.** Informational AI notices should not trigger additional consent prompts or communication requirements under ePrivacy, allowing user-friendly and legally sound implementation.
- **Develop joint guidance for startups through cooperation between the EU AI Office and the European Data Protection Board**. This should include template language and practical examples that fulfil all transparency obligations simultaneously.
- **Promote standardisation and interoperability.** The Commission should support the creation of common metadata and labelling standards for AI outputs to enable consistent and scalable compliance.

2.2 Data Access and Reuse

The interplay between the AI Act, the GDPR, and the ePrivacy Directive creates uncertainty for companies seeking to use data responsibly to train, test and improve AI systems. The AI Act requires providers to ensure that training data is high-quality, representative and free of bias, which in practice often means analysing or processing sensitive personal data. However, the GDPR and ePrivacy Directive impose strict conditions on processing such data, including limitations on reuse, purpose changes, and consent collection.

These frameworks are not yet aligned with the continuous learning and development cycles that characterise AI innovation. As a result, providers struggle to determine when and how personal or sensitive data may be lawfully used for bias detection, retraining, or model improvement. Particularly for startups and SMEs, this lack of clarity creates both compliance risks and innovation barriers. Many young AI companies rely on small, evolving datasets to refine their models. The current legal norms restrict their ability to reuse data for essential quality control and fairness checks, while demanding deletion of datasets that could be necessary for long-term monitoring. These combined constraints slow down AI improvement cycles, increase legal costs, and discourage experimentation. Ultimately, the absence of clear and practical rules for lawful data reuse puts European startups at a competitive disadvantage compared to ecosystems with more innovation-aligned data frameworks.

Policy Recommendations

- **Align AI Act and GDPR requirements** by replacing the “strictly necessary” standard in Article 10 (5) AI Act with the GDPR’s established “necessary” standard,

ensuring that bias detection and monitoring remain legally permissible throughout an AI system's lifecycle.

- **Recognise bias correction and algorithmic improvement as legitimate processing purposes** under GDPR Article 6 and Article 9 (2 lit. g,j), provided appropriate safeguards (e.g. pseudonymisation, purpose limitation, access controls[1]) are implemented.
- **Enable responsible data reuse** by clarifying that personal data collected for one purpose may be lawfully repurposed for AI training and testing when this serves compliance with the AI Act or demonstrable safety improvements.
- **Modernise ePrivacy provisions** to permit low-risk data collection (e.g. telemetry, performative analytics) without explicit consent, where such processing is necessary to ensure security, accuracy or fairness of AI systems.
- **Expand the concept of regulatory sandboxes** to include controlled environments for data reuse and bias testing, where startups can process sensitive data under supervision and with appropriate safeguards.
- **Issue joint guidance from the European Data Protection Board and the AI Office** clarifying lawful bases for data use under the combined framework, reducing uncertainty for startups while maintaining strong privacy protections.

2.3 Compliance Burden and Overlap

European AI startups face an increasingly complex compliance landscape, with overlapping and sometimes redundant obligations across the legal norms. Each framework requires extensive documentation, record-keeping, and assessments to demonstrate compliance. For instance, GDPR mandates a Data Protection Impact Assessment (DPIA) for high-risk data processing, while the AI Act introduces a Fundamental Rights Impact Assessment (FRIA) for high-risk AI systems, while covering largely similar risk dimensions. At the same time, both laws require technical documentation, auditability, and incident reporting. These parallel processes not only increase administrative burdens but also lead to uncertainty about which assessment or authority takes precedence.

For startups with limited resources, this fragmentation turns compliance into a major operational challenge and translates into disproportionate costs. Generally, startups lack the in-house legal or compliance departments that larger firms can rely on, forcing founders or engineers to spend valuable time on paperwork and overlapping filings instead of product development. Redundant assessments, like DPIA and FRIA, or separate reports for AI incidents and data breaches can double the workload without improving accountability. The financial impact is significant: for high-risk AI systems, compliance preparation alone can absorb tens of thousands of euros, effectively

[1] Art. 89 GDPR.

excluding smaller innovators from regulated markets. This imbalance risks consolidating market power among large incumbents while pushing early-stage AI ventures to relocate or delay product launches due to regulatory uncertainty.

Policy Recommendations

- **Integrate risk assessments.** Allow a single, comprehensive AI and Data Protection Impact Assessment that satisfies both FRIA and DPIA requirements. The European AI Office and the EDPB should jointly develop templates to ensure consistency across Member States.
- **Streamline documentation.** Permit startups to maintain a unified compliance file combining AI Act and GDPR documentation, accepted by all relevant authorities, rather than duplicating technical reports.
- **Establish one-stop reporting.** Introduce an EU-wide single reporting channel for digital compliance incidents, that is covering data breaches, AI system failures, or fundamental rights concerns, to prevent redundant notifications across regulators.
- **Simplify consent and user interaction.** Promote a harmonised, one-consent interface that satisfies both GDPR and ePrivacy obligations, allowing startups to implement uniform consent management across services.
- **Apply proportionality for SMEs.** Embed proportional documentation and audit requirements directly into the AI Act's implementation guidance; acknowledging that smaller providers can demonstrate compliance through simplified procedures.

2.4 Legal Fragmentation and Regulatory Conflicts

Despite the EU's objective of a harmonised digital single market, the interplay between the AI Act, the GDPR and the ePrivacy Directive still results in significant fragmentation. The ePrivacy Directive remains implemented differently across Member States, creating divergent consent, cookie and communications rules. Meanwhile, GDPR enforcement varies between national data protection authorities, and the AI Act introduces a new set of market surveillance and sectoral regulators, without a clear one-stop-shop mechanism for cross-border AI providers. This patchwork increases compliance complexity and produces regulatory overlaps, especially where data protection, AI governance and communications privacy intersect.

Companies often face uncertainty about which rule applies or which authority is competent, for instance when processing personal data to fulfil AI transparency. These inconsistencies undermine legal certainty and undermine the EU's objective of a coherent and consistent digital regulatory framework. For AI startups and SMEs,

regulatory fragmentation translates directly into cost, confusion, and slower market entry. Young companies developing cross-border services must navigate different interpretations of ePrivacy and divergent supervisory practices under GDPR. The absence of a clear coordination mechanism between AI, data-protection and telecommunications authorities creates the risk of parallel investigations and conflicting guidance. This environment discourages startups from scaling EU-wide and deters international investors who view regulatory unpredictability as a structural risk. Fragmentation also enables larger incumbents to maintain compliance advantages. Without streamlined supervision and uniform interpretation, the single market becomes fragmented into multiple compliance zones, effectively limiting the capacity of especially startups to grow across borders.

Policy Recommendations

- **Ensure cross-regulatory coherence.** Through the Digital Omnibus, align the AI Act, GDPR and ePrivacy frameworks by removing contradictions and clarifying their hierarchy where obligations overlap. Processing activities required for AI compliance should automatically qualify as lawful under GDPR.
- **Create a one-stop-shop for AI regulation.** Establish a coordinated supervisory mechanism modelled on the GDPR's lead-authority principle, empowering the EU AI Office to act as a central coordination point for cross-border AI compliance.
- **Modernise and harmonise ePrivacy rules.** Replace the outdated directive with a directly applicable regulation to eliminate national divergences and align consent, metadata and communications rules with the GDPR's terminology and principles.
- **Clarify legal bases and primacy.** Define how obligations under one regulation (e.g. AI Act transparency or safety monitoring) interact with privacy rules. The Digital Omnibus should explicitly state that compliance with the AI Act constitutes a "legal obligation" under GDPR Article 6(1)(lit. c).
- **Strengthen institutional coordination.** Create a Digital Regulation Coordination Forum bringing together the European AI Office, the EDPB and national communications regulators to issue joint guidance and resolve cross-regime conflicts before they reach enforcement.
- **Promote mutual recognition.** Ensure that AI certifications, assessments or approvals obtained in one Member State are automatically recognised across the EU to reduce duplication and support market scalability.

2.5 Open-Source and Innovation Impact

The combined application of the AI Act, GDPR and ePrivacy Directive risks creating unintended barriers for open-source development and early-stage innovation. While the

AI Act formally excludes non-commercial open-source components from its scope (Recital 12), it remains unclear where the line between non-commercial and commercial activity is drawn. The AI Act's broad definition of "providers" could capture open-source developers and research organisations, subjecting them to obligations meant for commercial deployers. At the same time, strict data-protection and consent rules make it difficult to use or share datasets essential for research and model improvement. For startups, open-source models and shared research tools are essential for innovation and competitiveness. Broad or unclear regulations may discourage small teams from using or releasing open-source components because of legal uncertainty and high compliance costs. This reduces collaboration between startups, researchers and civil society and risks shifting innovation towards large proprietary platforms. Without clear guidance and a consistent interpretation of these rules, the framework could unintentionally slow down the open innovation that drives Europe's AI ecosystem.

Policy Recommendations

- **Exempt non-commercial open-source development.** Clarify that releasing AI models or code under an open licence does not constitute "placing on the market" and is therefore outside the AI Act's provider obligations.
- **Broaden the research exemption.** All academic, pre-commercial and collaborative AI experimentation should remain outside the AI Act's scope until systems are deployed commercially.
- **Introduce a liability safeguard.** Limit the responsibility of non-commercial developers for downstream uses of open models; compliance duties should rest with commercial deployers.
- **Clarify GDPR application for AI research.** Confirm that personal-data processing for AI development and testing qualifies as "scientific research" under Art. 9 (2 lit. j) GDPR, provided strong safeguards such as pseudonymisation and ethical oversight are in place, to ensure consistent interpretation across Member States.
- **Expand innovation sandboxes.** Include open-source AI projects to allow supervised testing and collaboration under regulatory oversight.
- **Support open compliance tools.** Fund free, open-source templates for DPIA/FRIA, bias testing and documentation to reduce costs for SMEs and researchers.
- **Maintain structured dialogue.** Create a regular consultation forum between the AI Office, research institutions and open-source foundations to align rules and standards.

3. Cybersecurity and NIS-2 Alignment

AI providers are increasingly subject to the NIS-2 Directive, the AI Act and, in some cases, the Cyber Resilience Act. Each framework sets separate rules for security, incident reporting and risk management, often with different definitions, timelines and authorities. The lack of coordination leads to duplicated reporting, conflicting requirements and unclear thresholds for notification. For startups and SMEs, this overlap creates disproportionate costs. Small teams must maintain parallel monitoring systems and may need to report a single incident to several regulators. Such complexity discourages innovation in security-sensitive applications and diverts resources from development to compliance.

Policy Recommendations

- **One-Stop Incident Reporting:** Create a single EU gateway so one report fulfils all obligations under NIS-2, the AI Act and the CRA.
- **Harmonised Security Standards:** Issue joint ENISA and AI Office guidance on risk management, logging and vulnerability handling.
- **SME Proportionality:** Exempt micro and small enterprises from extensive NIS-2 documentation; allow simplified self-assessments.
- **Aligned Terminology:** Standardise definitions of "incident", "vulnerability" and "critical service" across digital laws.
- **Shared Audits:** Allow one combined security audit or certification to meet multiple regimes.[2]
- **Regulatory Coordination:** Ensure structured cooperation between ENISA, the AI Office and national authorities for consistent guidance and enforcement.

4. Cyber Resilience (CRA)

The Cyber Resilience Act introduces security-by-design and CE-marking rules that overlap with the AI Act's conformity and risk-management obligations. Without alignment, AI software providers risk double certification: one for cybersecurity under the CRA and another for safety and fundamental-rights compliance under the AI Act. Unclear definitions of "products with digital elements" add further legal uncertainty. For startups, dual conformity assessments are costly and time-consuming, often delaying market entry. Ambiguous classification of AI software increases compliance risk and discourages innovation in safety-critical and embedded-AI applications.

Policy Recommendations

[2] ISO 27001 (NIS-2/CRA) and Annex VII (AI Act) outline comparable risk-management and documentation duties; mutual recognition could replace duplicate audits.

- **Unified Conformity Assessment.** Integrate CRA and AI Act assessments into a single modular procedure with one audit and one certificate.
- **Mutual Recognition.** Results of a CRA security evaluation should automatically count towards AI Act safety requirements where applicable.
- **Exclude stand-alone software AI applications from CRA obligations** unless they control hardware or network-critical functions.
- **Common Standardisation Path.** Mandate CEN CENELEC/ ETSI to draft joint harmonised standards for cybersecurity.
- **SME Support.** Offer reduced audit fees and access to EU-funded conformity-assessment vouchers for startups to meet CRA/AI Act requirements efficiently.
- **Coordinated Oversight.** Ensure national market authorities responsible for CRA and AI Act supervision cooperate through shared databases and inspection planning to minimise redundant checks.

5. Data Governance and Data Act

The Data Act aims to enable data sharing and interoperability but often overlaps with GDPR and AI Act obligations. It should, therefore, also be considered in the Digital Omnibus.

While the goal of the Data Act, in particular to reduce vendor lock-in when it comes to cloud data, it is our opinion that due to a clear definition, certain provisions risk undermining business models of European SaaS companies. Many of these providers, and particularly startups and scaleups, rely on yearly or even multi-year contracts. Due to a lack of a clear definition in Art. 2 of the Data Act, the granted short-term termination rights regardless of contract length, could undermine these long-term SaaS contracts and therefore threaten the sustainability of these business models.

Furthermore, startups depend on access to diverse datasets to build and improve AI systems, yet face legal uncertainty when data-sharing duties conflict with restrictions on personal or sensitive data. Inconsistent definitions of “data holder”, “user” and “recipient” (Art. 2 Data Act) complicates contracts and liability, while unclear technical standards make interoperability costly and unpredictable.

Without clearer alignment and practical guidance, the Data Act’s promise to foster innovation may instead create compliance burdens that small companies cannot realistically manage.

Recommended Simplification Measures:

- **Clarify definitions in Art. 2 of the Data Act.** In order to encourage innovation rather than obstruct it, we recommend that the Data Act clearly distinguishes between cloud data portability, which fosters open and competitive markets, and provisions that could undermine SaaS and AI business models. Without this level of precision, the regulation could inadvertently weaken the ecosystem it is intended to support.
- **Harmonise definitions.** Align the terminologies for "data holder", "provider" and "user" across the Data Act and AI Act to avoid overlapping roles and liabilities.
- **Proportionate Obligations.** Allow simplified or sectoral exemptions for startups providing non-critical data services, reducing reporting and technical documentation duties.
- **EU Data Portal.** Create a single European interface where businesses can manage sharing permissions, metadata and transparency documentation across legal frameworks.
- **Cross-Regime Guidance.** The Commission should publish joint interpretation notes explaining how Data Act obligations interact with GDPR lawful bases and AI Act data-quality rules.

6. Institutional Coordination and Future Governance

The EU's digital rulebook delegates supervision to multiple authorities: data-protection agencies, cybersecurity regulators, market-surveillance bodies and the European AI Office. Without structured coordination, companies face fragmented oversight, divergent guidance and inconsistent enforcement. Existing cooperation mechanisms, such as the EDPB under GDPR, cover only part of the landscape. The AI Act introduces a new network of national competent authorities but lacks a clear cross-regulatory integration mechanism with data and cyber regulators. For startups, navigating this multi-layered supervision is confusing and time-consuming. Receiving conflicting advice from different authorities can delay compliance planning and deter cross-border expansion. Multiple audits or reporting obligations drain resources that smaller actors cannot spare. The absence of a unified contact point creates uncertainty over where to seek guidance or file notifications, especially for companies operating in several Member States.

Policy Recommendations

- **European Digital Coordination Forum.** Establish a permanent structure connecting the AI Office, the EDPB, ENISA and national regulators to issue joint guidance, coordinate enforcement and share data.

- **One-Stop Contact Point.** Allow companies to interact with a single lead authority for all major digital-law obligations, similar to GDPR's lead-supervisory model.
- **Unified Reporting Infrastructure.** Develop an EU-level portal for compliance filings, incident notifications and conformity documentation accessible to all relevant regulators.
- **Mutual Recognition of Audits.** Ensure that compliance verifications or certifications approved by one competent authority are recognised EU-wide.
- **Annual Joint Guidance Cycle.** Require the main EU digital regulators to publish coordinated annual guidance summarising enforcement priorities and cross-law interpretations.

7. Towards a Unified Digital Single Market for Innovation

Europe's digital competitiveness depends on a regulatory environment that protects citizens while enabling innovation at scale. The growing overlap between digital laws risks fragmenting the single market and discouraging investment. Without structural simplification, startups face cumulative compliance costs and persistent legal uncertainty, undermining Europe's global competitiveness. Fragmentation also hinders investors, who perceive complex regulatory frameworks as high-risk. A more coherent and harmonised EU rulebook would accelerate time-to-market, reduce legal overhead and strengthen the participation of European SMEs in global AI value chains.

Policy Recommendations

- **Introduce an Innovation Test.** Assess the impact of all new EU digital laws on startups and SMEs before adoption.
- **Make simplification permanent.** Establish a recurring review to align and streamline digital legislation regularly.
- **Ensure proportional enforcement.** Require regulators to consider company size and innovation potential when applying supervision or sanctions.
- **Enable standards-based compliance.** Recognise harmonised technical standards (e.g. ISO, CEN/ CENELEC) as evidence of compliance across multiple acts.
- **Advance a unified EU framework.** Use the Digital Omnibus to move towards a single, coherent European rulebook for AI, data and cybersecurity.
- **Right to Error.** Introduce a mechanism allowing startups to correct first-time compliance mistakes before penalties apply, provided no harm or intent is involved.

- **Once-only principle.** Apply a single-submission rule for compliance documentation across the digital laws, enabling authorities to share data instead of requiring repeated filings.
- **SME transitional period.** Provide longer adaption timelines for SMEs to meet new digital requirements without compromising innovation.

About the European AI Forum EAIF:

The European AI Forum (EAIF) is the umbrella organisation of 13 national European AI associations and clusters. Combined, we represent over 3000 members, making us the largest European AI organisation. We represent members such as SMEs, corporates, organisations and individual experts in AI.

Contact:

info@eaiforum.org