Meta

14 October 2025

Meta Submission: "Call for Evidence – Digital Omnibus"

Digital Package on Simplification

Introduction

Europe stands at a crossroads. As highlighted by former European Central Bank President Mario Draghi, the multiplication of digital regulators, the accumulation of EU-level legislation, its increased complexity, and the challenges companies face in implementing the rules are having a detrimental impact on Europe's competitiveness. Today's economic landscape shows that Europe can no longer afford to limit its potential. A sense of urgency is needed. A different path, built on speed, scale, and intensity is required.

The announcement and launch of the Digital Simplification Package represents a once in a generation opportunity for Europe to address past regulatory missteps. The Digital Omnibus is an encouraging first step and it is essential that this exercise has ambitious objectives in order to address the real challenges created by Europe's regulatory regime. As companies continue to grapple with a complex web of digital legislation and regulators, the goal of lowering unnecessary administrative costs for businesses is a laudable task, and one that we strongly support. However, a slight easing of the compliance burden will not unlock the innovation Europe needs to adapt to a fast-changing technological landscape.

The European Commission ("**the Commission**") must be ambitious in order to support its objectives of competitiveness, growth and exporting of European values. The Digital Omnibus, and the upcoming Digital Fitness Check, must go beyond the simple easing of selective administrative compliance burdens. It must seek to identify and rectify those sections of the EU's digital rulebook that have a true role in limiting digital innovation in Europe. A failure to act convincingly could leave Europe in a position it may never recover from and find itself left behind in the global digital race.

To ensure Europe creates a future digital regulatory environment that is both competitive and simplified, we encourage the Commission to take the following actions:

- **Embed Innovation** - Explicitly include innovation as a core objective for digital regulation and regulators
- **Artificial Intelligence ("AI")** - Pause the implementation and enforcement of the EU AI Act so that it may be reformed
- **Privacy & Data Protection** - Reform the EU Data Protection and Privacy regime to create a modernised and innovation driven framework

Meta

Summary of Recommendations

Pause the Implementation and Enforcement of the EU AI Act

Many European CEOs have signed initiatives asking for a moratorium on enforcement of the EU AI Act (**"AIA"**) to allow for a thorough simplification process to occur. Governments from Germany, Sweden, Denmark, Poland and Czechia have raised the need to simplify the AI regulatory regime to restore European competitiveness. The EU AIA's late-stage addition of complex rules for General Purpose AI Models (**"GPAIM"**) threatens to deter investment, slow AI adoption, and undermine Europe's technological leadership. These GPAIM provisions introduce unnecessary complexity and risk stifling innovation at a pivotal moment. At the same time, the AIA's disproportionate high-risk framework could further restrict the development and deployment of beneficial AI technologies. Coupled with a fragmented governance structure that fosters regulatory divergence and legal uncertainty, the AIA risks failing its core objective of harmonising AI rules across the EU. Removing the GPAIM rules, recalibrating the high-risk framework, and streamlining oversight are essential to ensure the AI Act truly supports Europe's competitiveness and innovation in AI.

To ensure the AIA achieves its objectives, several key reforms are essential. To make these changes possible, it is critical to first pause the implementation and enforcement of the Regulation. This pause will provide the necessary time to undertake meaningful reforms without risking the EU falling behind in the global AI race.

- **Remove the GPAIM Regime**: Refocus the AIA on regulating AI use cases rather than underlying technologies, ensuring the framework remains adaptable and supportive of innovation.
- **Recalibrate the High-Risk Framework**: Revise the high-risk provisions to ensure a proportionate, balanced approach that addresses genuine risks without unnecessarily hindering economic growth or technological progress.
- **Preserve Established Copyright Norms**: Avoid creating unnecessary complexity and uncertainty by adding provisions on extraterritoriality that goes against established copyright law and jurisprudence
- **Streamline Governance**: Establish a unified and efficient enforcement mechanism, reducing the number of national authorities and creating a single point of contact for compliance to enhance legal certainty and reduce administrative burdens.
- **Clarify Batteries Requirements**: Simplify the Batteries Regulation to ensure Europe preserves its leadership in AI wearables
- **Embed Innovation in Regulators' Mandates**: Explicitly include innovation as a core objective for all digital regulators, ensuring that the regulatory environment actively supports technological advancement and economic competitiveness.

Meta

Reform the EU Data Protection & Privacy Regime to Create a Modernised Framework

The EU's data protection and privacy framework - anchored by the General Data Protection Regulation (**"GDPR"**) and the ePrivacy Directive (**"ePD"**) - is foundational for Europe's digital economy and society. However, rapid technological change and the rise of data-driven innovation have exposed significant shortcomings, including regulatory complexity, absolutist interpretations, excessive compliance burdens, and fragmented enforcement. The EU's policy framework should place innovation and technology development at its core. Regulatory frameworks must support - not hinder - the growth of digital markets and emerging technologies. A risk-based, future-proof approach to regulation is essential, enabling experimentation and investment in AI, privacy and safety-enhancing technologies (**"PETs"**), and cross-border digital services. The EU's ability to foster homegrown digital champions and become globally competitive depends on agile, innovation-friendly policies that encourage both large-scale and grassroots technological advancement. Digital regulators also play a critical role in fostering innovation as they must interpret and implement the legal framework in ways that make the EU's economic and policy goals possible, that encourage experimentation, technological progress, provide clarity, and flexibility where rigid and siloed applications stifle economic development. By acting as active facilitators rather than mere enforcers, regulators can help innovation and emerging technologies reach their potential, including by fostering fundamental rights and public trust.

By fostering an environment where there is legal certainty that data can be leveraged for innovation, new business models, and improved services, the EU can unlock significant economic potential and drive the growth of a thriving macroeconomy. Today, innovation in the EU is snarled up by a deeply fragmented data regulatory environment far from the harmonised Digital Single Market (**"DSM"**) promised by policymakers. The failure of macro-EU policies to realise the strategic importance of data to the future of EU competitiveness has resulted in an absolutist regulatory regime uninterested, or incapable, of balancing both strategic national and transnational priorities with the protection of fundamental rights. Policies should empower individuals with control and transparency, while also enabling businesses to responsibly harness data for societal and economic benefit.

Moreover, the free flow of data across borders is essential for innovation, competitiveness, and the development of new technologies, yet legal uncertainties in recent years - stemming from national data protection authority (**"DPA"**) decisions that challenge the GDPR's risk-based approach, ignore its derogations, and introduce impractical requirements - have complicated cross-border transfers. These barriers fragment the DSM, limit opportunities for startups and small-medium sized enterprises (**"SMEs"**), and hinder the EU's global competitiveness. Industry leaders and privacy professionals agree that seamless, secure data transfers are crucial for innovation, particularly in areas central to the EU's digital priorities, such as AI and cybersecurity. The EU should therefore prioritise removing restrictions on data flows to enable dynamic data ecosystems, support research and development (**"R&D"**), and drive growth.

To unlock the EU's digital potential and foster responsible innovation, reform of the data protection and privacy framework is needed to restore balance, embed proportionality, and harmonise interpretations and enforcement.

- **Promote Innovation and Restore Proportionality**: Amend the GDPR to explicitly include innovation and economic interests as objectives, and embed a risk-based approach to ensure obligations are tailored to actual risks, not applied uniformly to all processing activities.
- **Reduce Excessive Compliance Burdens:** Scale back documentation and compliance requirements according to risk, provide clear guidance on data subject requests, and encourage standardised, user-friendly privacy notices to focus on meaningful information for citizens.
- **Centralise Interpretation and Harmonise Enforcement:** Establish a centralised EU body for consistent interpretation and guidance, harmonise enforcement across the GDPR, ePD, and other digital laws, and implement a unified breach reporting model to reduce complexity and legal risk.
- **Modernise Consent and Legal Bases:** Move beyond "consent absolutism" by allowing all GDPR legal bases for cookies and similar technologies, create exemptions for low-risk use cases, and recognise PETs as grounds for exemptions from consent.
- **Align with other EU Digital Laws:** Fully harmonise theGDPR and ePD with the AIA, Data Act, Data Governance Act (**"DGA"**), Digital Services Act (**"DSA"**), and Digital Markets Act (**"DMA"**), clarifying relationships and ensuring proportionality, transparency, and legal certainty across the digital regulatory landscape.

We also address the need for important reforms to the EU's cybersecurity framework in this submission, as well as the critical need to review the Batteries Regulation in order to maintain Europe's leadership in AI wearable.

Meta

1. Pausing the Implementation and Enforcement of the EU AI Act to Secure European Competitiveness

Initially designed as a risk-based, innovation-forward legislative framework, the AIA has become weighed down by political compromises, added vagueness and complexity, and protectionist implementation. All this threatens inward investment, EU's economic growth and technological leadership. This is particularly acute for the AIA's rules on GPAIM. If left unchecked, the GPAIM framework - introduced late in the AIA's negotiations - will undermine competitiveness, deter investment, and slow AI adoption at the very moment other global powers are accelerating ahead.

The evidence is clear. European startups and SMEs, already struggling under heavy compliance demands, view the AIA largely as a disproportionate barrier. Only 20% of founders expect a positive impact. Major European companies have urged Brussels to simplify digital regulation, including the AIA, and over 70 publicly traded firms now cite the AIA as a business risk in filings to the US Securities and Exchange Commission (**"the SEC"**). These concerns echo those of Mario Draghi, which underscores the structural weaknesses of Europe's innovation ecosystem and how cumulative regulatory load on advanced computing threatens to shift R&D investment abroad. Meanwhile, the concerns which animated the inclusion GPAIM within the AIA - systemic AI risks and slow uptake in the absence of regulation - have not materialised.

In contrast, global peers are pursuing pro-innovation paths. The United States is prioritising removing regulatory barriers to AI innovation, and investing massively in AI infrastructure. The UK has embraced a flexible, innovation-driven regulatory model, and governments from Japan to India, China, Singapore, and Switzerland are focused on enabling opportunity, not constraining it. The EU's assumptions that new rules are needed and that these would set the global standard have proven to be misplaced. Instead, its approach is isolating the EU in an era when trust, competitiveness, and rapid adoption define AI progress.

Europe must recalibrate. The AIA can only achieve its stated ambitions if it respects the territorial integrity of its allies, avoids overreach, takes an evidence-informed approach to identify net new risks, balances mitigating those risks with facilitating innovation, and creates an environment in which homegrown champions can thrive. This begins with a fundamental re-evaluation of the GPAIM regime - a regime whose significant flaws and excessive burdens risk severely undermining Europe's competitiveness at a time when bold, unified leadership is essential.

In addition, the Commission must urgently address the disproportionate nature of the high-risk framework of the AIA, ensuring they are recalibrated to support innovation rather than stifle it. Equally critical is the need to overhaul the governance framework at both the EU and Member

State levels. The current approach, where individual Member States designate more than ten separate authorities to oversee AIA compliance within a single country, is a recipe for fragmentation, regulatory power struggle and administrative chaos. Without decisive reform, these issues will not only impede progress but also jeopardise Europe's position on the global stage.

1.1 The GPAIM Regime: Why Regulating Technology Itself Is Ineffective

The relentless pace of technological advancement - especially in AI - poses a profound challenge for policymakers. The reality is clear: prescriptive, *ex-ante* regulation simply cannot keep up with innovation. This is precisely why Europe's peers have eschewed this approach, in particular, regarding GPAIM. Technology evolves rapidly, while regulation should provide agile but stable, outcome-focused guardrails - not rigid, technical prescriptions.

The GPAIM Regime: Outdated and Misaligned

The AIA's GPAIM regime is a striking illustration of why regulating technology itself is fundamentally flawed. Already to a large extent outdated, the GPAIM provisions in the AIA were introduced late in the legislative process, reacting to external developments rather than grounded in scientific evidence or international consensus. The provisions were introduced after the Commission's original Impact Assessment had closed, and lacked any quantitative analysis of implementation costs or feasibility. Moreover, this approach diverges sharply from the original intent of the AIA, which was to regulate the use of AI systems based on risk, not to police the underlying technology. The result is a regime that is misaligned with both the needs of the market and the realities of AI innovation. Attempts to regulate specific technical parameters - such as using floating point operations (**"FLOPs"**) to classify AI models - may be rendered obsolete almost as soon as they are conceived in a nascent technology environment. Recent breakthroughs in model architecture and training efficiency have dramatically reduced the compute required for advanced AI. Notably, in the past year, there are several Chinese GPAIM reportedly as performant as the most capable US and EU models, that have achieved state-of-the-art performance with far less compute than previously imagined.

The Futility of Technical Thresholds in AI Regulation: The Complexity of GPAIM Development

The development of GPAIMs is a complex, multi-stage process involving large-scale pre-training on trillions of tokens, fine-tuning for specialised capabilities, reinforcement learning from human feedback, and ongoing evaluation against evolving benchmarks. This process often relies on compute resources spanning heterogeneous infrastructure, including various graphics processing unit (**"GPU"**) architectures, precision levels, and adaptive

optimisation strategies, which makes precise FLOP accounting inherently uncertain. For many providers, each training run could consume weeks of cluster time and incur millions of Euros in energy and hardware amortisation costs. Retrofitting existing systems with the logging infrastructure contemplated by the AIA could necessitate bespoke telemetry pipelines, representing a significant engineering investment - potentially costing millions for a single state-of-the-art GPAIM. Moreover, capabilities in these models emerge unpredictably from the interplay between data, architecture, and optimisation, with an unpredictable relationship between compute expenditure and resulting capability. The training datasets themselves are generally highly heterogeneous, comprising web data, licensed corpora, and synthetic content, which renders comprehensive data auditing technically impracticable at scale. Consequently, the regulatory assumption that AI development follows predictable, measurable, and controllable processes is fundamentally at odds with the empirical realities of engineering practice.

The Inadequacy of Compute-Based Risk Metrics

This mismatch underpins the core flaw of the AIA GPAIM framework in that it creates an *ex-ante* systemic-risk presumption at 10^25 FLOPs. Research from Epoch demonstrates that estimates can diverge by significant percentages depending on factors like precision and sparsity, and even the European AI Office (**"AIO"**) guidelines concede a 30% margin of tolerance. Given the hardware-level logging, data storage, and verification audits for FLOP measurement contemplated by the AIA, the costs could be substantial, and the ongoing engineering effort required to maintain profiling scripts and perform sanity checks for each major training run is far from trivial, regardless of the size of the provider. The challenge could be further compounded when third-party models are incorporated during pre-training, as compute attribution is generally not feasible without access to proprietary telemetry. Given that at present there is no harmonised methodology or tooling for cross-framework FLOP measurement, the result is a regulatory trigger that is both technically unmeasurable and administratively burdensome, with compliance costs measured in millions of Euros rather than tokens. This is clearly illustrated by the fact that while state-of-the-art models such as Gemini 2.5 Pro and GPT-5 currently lead 2025 benchmarks, more efficient architectures like DeepSeek R1 and Stanford's S1 reasoning model can achieve comparable reasoning performance at a fraction of the training cost, thereby undermining the validity of compute-based risk frameworks. Publicly documented examples (e.g. DeepSeek R1's MoE architecture, which purportedly activates only a fraction of its parameters, and Stanford's S1 approach using test-time scaling) suggest that it is feasible to approach, or even match, the reasoning performance of models like Gemini 2.5 Pro or GPT-5 with much lower inference compute. That undermines any simple "risk equates to raw compute budget" framework, because a malign actor could exploit efficient inference architectures rather than own an entire exascale cluster.

The Chilling Effect on Innovation and Competitiveness

Anchoring compliance to specific technical characteristics risks creating a chilling effect on the very innovation Europe aims to promote. Such requirements are likely to deter new entrants and slow technological progress, undermining the region's competitiveness. Regulating the underlying technology, rather than its use or outcomes, is not only ineffective but ultimately counterproductive. To ensure regulation remains relevant, adaptable, and supportive of innovation, it is essential to adopt a technology-neutral approach that focuses on the responsible use and real-world impacts of AI systems.

1.1.1 High Cost, Low Impact, and No Real Risk Reduction

The flaws of the GPAIM regime in the AIA extend far beyond its well-intentioned, but unfortunately fatally flawed, attempt to regulate technology itself. Even if the pace of innovation could be matched by legislation, the regime's rules are fundamentally complex, unclear, resource-intensive, and often ambiguous, demanding extensive documentation, reporting, and technical disclosures that are both costly and difficult to implement in practice - while failing to deliver on their most important promise: reducing marginal risk.

Technical Misalignment

This has been a sustained criticism of the AIA since it was finalised, including by both signatories and non-signatories of the Code of Practice for providers of GPAIMs. These provisions continue to rest on incorrect technical assumptions about how AI models are developed and evaluated with the only real outcome being that they represent a significant barrier to enter the market, diverting resources away from research, development, and responsible deployment of AI.

Fundamentally, the GPAIM rules in the AI Act suffers from four systemic flaws:

1. A duplicative regulation at upstream and downstream levels;
2. Reliance on arbitrary technical metrics unrelated to risk;
3. Dependence on "standardised" methodologies that do not yet exist; and
4. Compliance obligations that are infeasible given the current state of AI science and engineering.

Redundant Compliance and Missed Opportunities

The dual approach of regulating both upstream and downstream in the AIA imposes overlapping compliance obligations on both model providers and system deployers. As a result, resources are diverted to documentation and reporting, rather than on effective risk mitigation.

Ultimately, this approach fails to deliver better outcomes for people or society, while increasing costs and slowing innovation across the AI ecosystem. A more effective framework would focus regulatory efforts where risks may actually materialise - i.e., at the system level - ensuring clarity, efficiency, and real-world impact. It would also rely upon the existing, extensive applicable EU regulation - data protection, consumer protection, antitrust, and sectoral safety regulations - available to address potential AI-related harms.

Structural Problems Require Structural Solutions

The AIA's vague and burdensome GPAIM rules do not necessarily translate into meaningful risk mitigation. The most immediate risks associated with AI do not stem from the technology itself, but from how it is used in real-world applications. By attempting to regulate both upstream and downstream simultaneously, the AIA creates a disproportionate, fragmented and inefficient regulatory regime. This dual approach dilutes accountability, confuses responsibilities, and ultimately fails to address the actual sources of potential marginal risks.

These structural problems cannot be resolved through guidance, delegated acts, or any "band-aid" targeted reform. The structural problems of the AIA's GPAIM rules stem from fundamental infirmities embedded in the regulatory architecture of the AIA itself.

1.1.2 The GPAIM Framework's Safety Theater Is Compliance Without Safety

These structural flaws culminate in "compliance without safety." The AIA's requirements on GPAIM systematically fail to address actual AI safety risks while creating the illusion of comprehensive governance. FLOPs thresholds target computational expenditure rather than harm potential - a hypothetical large model trained with massive compute for language translation poses minimal risk, while smaller models intentionally trained on data optimised for influence operations could result in significant harm when used in an AI system.

Lack of Standards and Unclear Benchmarks

The AIA mandates the adoption of "standardised protocols and tools reflecting the state of the art." However, such standards have not yet been established, and there is currently no consensus within the field regarding appropriate metrics or thresholds for evaluating advanced AI models. As noted by the Frontier Model Forum, no single benchmark is capable of adequately capturing the systemic risk potential associated with these technologies. The unpredictable nature of emergent behaviors and the context-dependent performance of these systems make *ex-ante* risk quantification highly speculative. Furthermore, the AIA imposes post-market monitoring obligations that extend indefinitely, without a clearly defined temporal scope. As a result, the AIA effectively mandates compliance with standards that are still the subject of ongoing scientific research, imposing significant costs even on the largest AI providers.

Documentation Burdens Without Safety Gains

Documentation mandates generate compliance artifacts unrelated to threat prevention: internal technical specifications provide no protection against model misuse, adversarial attacks, or inappropriate deployment contexts. "Systemic risk evaluation" without defined standards incentivises performative assessments over substantive safety engineering, while cybersecurity requirements focus on infrastructure protection without addressing AI-specific attack vectors like prompt injection, data poisoning, or adversarial examples. Annex XI of the AIA requires comprehensive internal documentation covering training procedures, evaluation methods, and compute metrics, while Annex XII mandates that certain information be made publicly accessible for downstream providers. The AIA further stipulates that this documentation must be kept “up-to-date,” yet it provides no materiality threshold or temporal guidance for updates. Legal analysis by Mayer Brown highlights the absence of clear criteria for when and how documentation should be revised, raising the risk of perpetual revision cycles. Additionally, these requirements create unavoidable intellectual property conflicts, as disclosures may expose proprietary architectures and optimisation techniques.

The lack of international standards defining adequate documentation for AI models further complicates compliance. Moreover, the AIA imposes transparency obligations on GPAIM providers, with the transparency template emerging as a significant concern. The AIA provides minimal detail, merely requiring providers to publish a “sufficiently detailed summary” of training data using a template developed by the AIO. This vagueness has enabled regulatory overreach, as the current template demands disclosure of commercially sensitive information. The template was developed with limited stakeholder input and adopts a one-size-fits-all approach that is ill-suited to the diversity of AI models. It also exceeds the legislative intent, risking the stifling of competitiveness and innovation.

Incompatibility with Open Source

In cases where AI models integrate third-party components, providers may encounter considerable technical barriers in attributing compute usage and maintaining comprehensive documentation. Recital 108 and Article 53(3) of the AIA assign ongoing responsibility to the integrating provider, even in cases where upstream data sources and compute budgets are unknown or inaccessible. In reality, fulfilling the GPAIM rules’ traceability requirements across interconnected models could necessitate the creation of end-to-end data and compute provenance systems - technology that does not currently exist and could require millions of Euros to develop and implement. As such, the current GPAIM framework inadvertently penalises the collaborative development model that is foundational to Europe’s AI ecosystem, imposing fixed compliance costs that do not scale with the size or resources of the enterprise.

Open-Ended Cybersecurity Obligations

The AIA requires providers to ensure an "adequate level of cybersecurity," yet it does not define any specific technical baseline for compliance. AI-specific cybersecurity standards are still in the early stages of development and lack maturity. Establishing a robust cyber-resilience posture for AI models - including model-weight encryption, access controls, intrusion detection, and secure inference application programme interfaces (**"APIs"**) - could demand significant investment, potentially amounting to millions of Euros in tooling and substantial dedicated full-time resources for ongoing monitoring and reporting. Furthermore, standards organizations such as ISO/IEC currently offer no guidance regarding incident severity or response deadlines. As a result, organisations face open-ended expenditures with no clear path to measurable compliance certainty. To address these challenges, it is essential that EU regulations are explicitly aligned with internationally recognised standards, frameworks and best practices.

To ensure interoperability and efficiency, regulatory obligations should be mapped to accepted standards, ensuring that compliance aligns with EU regulatory requirements. Standards organisations and regulators should jointly define incident severity levels and response deadlines, reducing uncertainty and enabling effective cross-border collaboration.

Safety Theater and Structural Disadvantage

The result is a regulatory framework that diverts millions of Euros and scarce engineering talent from proven safety measures toward bureaucratic exercises that enhance compliance documentation without necessarily improving safety outcomes. The GPAIM regime institutionalises safety theater while systematically undermining the technical collaboration and resource allocation necessary for genuine AI safety.

The AIA's obligations on GPAIMs depend on measurement and documentation infrastructures that do not yet exist. They contemplate recurring monetary and engineering costs - measured in millions of Euros per model release and tens of full-time technical staff - that likely neither correlate with risk nor enhance safety. By embedding technically unrealisable requirements into binding law, the EU has risked converting its flagship AI regulation from a competitive advantage into a structural disadvantage - an innovation ceiling disguised as a safety floor.

1.1.3 Reach of the EU Copyright Law and Extraterritoriality

The growing complexity and uncertainty resulting from overlapping and conflicting regulations significantly impede technological innovation and AI development in Europe. When the AIA seeks to alter the scope of the Copyright Directive, it introduces further legal ambiguity, risks regulatory overreach, and undermines established legal principles and jurisprudence. Such changes stifle innovation making it essential to maintain clear, stable, and predictable legal

frameworks that support technological progress in the EU. The AIA contains provisions and references in the recitals (Recital 106) that require the implementation of a copyright policy on compliance with EU copyright law regardless of the jurisdictions in which copyright-relevant acts underpinning the training of GPAIM's takes place. This seeks to effectively expand the scope of EU copyright law beyond the EU territory. This expansion is inconsistent with established international legal principles and jurisprudence. Copyright law is inherently territorial and primarily regulates activities – such as AI model training – according to the laws of the place where they occur. A recital should not be used to override fundamental European copyright principles. This concern arises from Article 2(1)(a), which states that the AIA applies regardless of whether a provider is established within the EU or in a third country. This approach creates legal uncertainty and compliance challenges for AI developers, as it forces companies to address European copyright standards even when they lawfully trained models in countries with different copyright frameworks, potentially exposing them to conflicting legal obligations. We would recommend deleting the extraterritoriality provision to avoid regulatory confusion and ensure alignment with established international copyright law principles.

1.1.4 Recommendation

- **Remove the GPAIM regime (Chapter V, including accompanying Recital 106):** To ensure that regulation remains relevant, adaptable, and supportive of innovation, it is essential to adopt a technology-neutral framework that emphasises the responsible use and real-world impact of AI systems. In the context of the AIA, the Regulation should return to its original focus on regulating AI use cases, rather than the underlying technologies themselves. In particular, the GPAIM focused rules of the AIA should be removed - especially those outlined in Chapter V - to make this a reality.

1.2 The High Risk Regime: The Need to Enhance Proportionality

The high-risk framework established by the AIA is poised to play a pivotal role in shaping the trajectory of AI both within Europe and globally. While the AIA aims to promote safety and trust in high-risk AI systems, it also raises significant concerns regarding its preparedness, clarity, and proportionality. The accelerated legislative process has resulted in notable gaps, most prominently the absence of finalised technical standards and the risk of overly broad or fragmented interpretation. These deficiencies may impose disproportionate burdens on providers and potentially impede AI innovation within the EU. The Commission should address this by pausing the implementation and enforcement of the high risk rules to ensure a more proportionate, targeted, and economically balanced approach

Rushed and Unfinished Framework

One of the primary concerns is that the framework has been rushed and remains unfinished. The regime relies heavily on harmonised technical standards, to be developed by CEN and CENELEC, which are intended to provide clear and consistent compliance pathways. However, these standards will not be finalised in time for the scheduled implementation, leaving organisations without the necessary tools to ensure compliance and creating significant legal uncertainty. Moving forward without these foundational standards risks inconsistent enforcement and a fragmented regulatory landscape across Member States. In light of these considerations, it is imperative that the implementation and enforcement of the high-risk regime be suspended until robust standards and comprehensive guidance are firmly in place. Premature action risks undermining both innovation and legal certainty across Europe. This prudent approach echoes the clear warning issued by Draghi in his speech marking the one-year anniversary of his report on European competitiveness, underscoring the urgent need for policymakers to prioritise clarity and stability over hasty regulation.

Vagueness and Lack of Clarity in Requirements

Another major issue is the vagueness and lack of clarity in the AIA's requirements for high-risk AI systems, particularly those outlined in Articles 9 to 15 (risk management systems, data governance, documentation, record-keeping, transparency, human oversight, accuracy, robustness & cybersecurity). These provisions are drafted in broad and ambiguous terms, lacking the specificity necessary for consistent application across a diverse array of AI systems. Without clarity on the adoption of these rules, there is a substantial risk of overly expansive interpretation, which could place undue burdens on system providers and stifle innovation within the EU. If sufficient clarity is not achieved by the legislation, it will inevitably need to be achieved by the courts. This would significantly extend the period of uncertainty for the industry and increase the risk of diverging interpretations at Member State level, contrary to the AIA's core objective to create a harmonised and predictable regulatory environment for AI across the EU. To address this, the AIA should explicitly ensure that all obligations under the high-risk regime are subject to a proportionality test, requiring only those measures that are necessary and appropriate to the actual risks posed, and taking into account economic interests and benefits for society as whole. This approach would help the AIA achieve its objectives while supporting innovation and competitiveness within the European AI ecosystem.

Challenges with Territorial Scope

The territorial scope of the AIA also presents challenges. The AIA applies to systems "whose outputs are used in the EU," but this concept is not clearly defined. As a result, it is disproportionately difficult to manage the territorial scope, as it may be impractical or even impossible in some cases to monitor and implement processes that track whether an AI

system's output has been used in the EU. The law should therefore provide clarity on how organisations should determine when outputs are used in the EU, and recommend practical solutions, such as restrictions in an AI system's terms of use, to make the scope more proportionate and manageable.

Provider and Actor Obligations

Provider and actor obligations under the AIA, such as the implementation of a quality management system (**"QMS"**), logging, corrective action, and cooperation with authorities, are onerous and lack sufficient detail. There is uncertainty regarding the proportionality of these requirements, the allocation of responsibilities, and the level of documentation required to demonstrate compliance. It is recommended that all provider obligations be subject to a proportionality assessment, taking into account the size of the provider and the number of high-risk AI systems. In the absence of finalised standards, reliance on existing QMS frameworks should be permitted. Responsibilities for logging and corrective action should be clearly allocated, and the level of required documentation should be specified to avoid unnecessary administrative burdens.

Modification and Change Management

Finally, the AIA's provisions on modification and change management are unclear. An AI system may be brought into scope if it has been subject to "significant changes in their design" or a "substantial modification," but the interaction between these terms and the definition of "substantial modification" are not clear. This is particularly problematic regarding the thresholds for what constitutes a substantial change, the interaction with intended purpose and misuse, and the alignment with existing EU product safety law.

1.2.1 Classification of High Risk AI System Rules

It is crucial that classification rules are precisely calibrated to avoid placing undue burdens on AI innovation and competitiveness within the EU. Overly broad or ambiguous provisions risk stifling beneficial AI development, deterring investment, and weakening the EU's global position in AI. To meet the AIA's objectives without unintended negative consequences, high-risk classifications should be narrowly focused on AI systems that present genuinely significant risks. This ensures that regulation is targeted and effective, while allowing low-risk and beneficial AI applications to thrive. A proportionate, risk-based approach is essential to protect fundamental rights and foster innovation.

Within this context, two areas in particular require closer examination: biometric and employment-related classification rules. These categories cover a broad spectrum of technologies with varying risk profiles, and current rules may inadvertently capture systems that do not pose substantial threats. To maintain a balanced and effective regulatory

framework, we recommend targeted adjustments to the classification rules in these domains. Specifically, the following two rules warrant further scrutiny and refinement to better align with the AIA's risk-based approach.

High-Risk Biometric AI Systems

Annex III of the AIA is intended to identify AI systems that present significant risks, particularly in the context of "biometric" applications. However, the current provisions relating to biometrics are both unclear and overly broad, which may inadvertently encompass a wide range of biometric uses that do not, in practice, pose meaningful risks to fundamental rights, health, or safety. For instance, the definition of "remote biometric identification systems" is too narrow, potentially excluding only a small subset of low-risk applications, while innocuous uses - such as AI tools that identify public figures in photographs or sort user-applied tags - could be unnecessarily classified as high-risk despite presenting minimal risk. The broad drafting of biometric categorisation risks capturing systems that do not enable discrimination or other harms, and the provisions on "emotion recognition" fail to sufficiently distinguish between high-risk and low-risk use cases. Furthermore, inconsistencies in terminology, such as the use of "emotion recognition system" in Article 3 but not in Annex III, create additional uncertainty.

To address these issues, it is recommended that the biometrics provisions be clarified and narrowed to ensure they apply only to use cases that genuinely entail significant risks, as outlined in Annex III, points 1(a)-(c). Exemptions for low-risk biometric identification systems, such as those used for identifying public figures or sorting non-sensitive data, should be broadened. Clear thresholds should be established to define when biometric categorisation is considered high-risk, with a focus on systems capable of enabling discrimination or other significant harms. Additionally, the provisions on emotion recognition should be refined to exclude low-risk applications and terminology should be made consistent throughout the AIA.

Classification of AI in Employment

In the context of employment, the human resources sector is a major adopter of AI, but the current drafting of Annex III, paragraph 4, risks capturing a wide range of low-risk AI tools used in recruitment and employment. This could discourage innovation and the adoption of beneficial technologies due to the threat of disproportionate regulatory burdens. There are specific concerns that AI systems which do not influence decision-making, such as translation tools and scheduling assistants, may be classified as high-risk. Similarly, basic matching or filtering tools that do not involve profiling or evaluative functions could be unnecessarily regulated, and AI tools that support anonymisation or are used by candidates themselves, such as grammar checkers, do not present significant risks, but may nonetheless fall within scope. Even promotion decisions based on fixed, transparent criteria could be captured, despite not requiring interpretation or presenting risks to fundamental rights.

To mitigate these concerns, it is essential to establish clear and practical boundaries for the classification of high-risk AI systems in the employment context, focusing on applications that have a direct impact on fundamental rights, health, or safety. AI systems that do not participate in the decision-making process - such as translation tools, scheduling assistants, and matching solutions - should be explicitly excluded from the high-risk category. Tools intended to reduce bias, including anonymisation technologies, or those designed to support candidates, should not be subject to high-risk classification. Finally, AI systems used for promotion decisions should be excluded where they operate solely on the basis of fixed, transparent criteria that do not require interpretation.

1.2.2 Recommendations

- **Adopt a More Proportionate High-Risk Framework:** The high-risk regime within the AIA should be revised to ensure a proportionate approach to regulating AI use. Legislative measures should be limited to those that are necessary and appropriate to address the actual risks posed, while also considering economic interests and the broader societal benefits of AI. This balanced approach would enable the AIA to achieve its objectives without unduly hindering innovation or competitiveness within the European AI ecosystem.
- **Implement a Strategic Pause:** In light of the current challenges, it is crucial - consistent with the approach recommended for the GPAIM Regime - to temporarily pause the implementation of the high-risk framework. This pause would provide an opportunity for further stakeholder consultation, a thorough reassessment of the fragmented governance structure, and the development of clear, practical, and proportionate guidance at the EU level. Such measures are essential to enhance predictability and legal certainty, thereby fostering sustainable AI development and growth across the region.

1.3 Governance Regime of the AI Act

1.3.1 Fragmentation and Inconsistency in National Oversight

The AIA's current approach to governance at the Member State level allows each country to appoint multiple national competent authorities, including notifying and market surveillance bodies, to oversee the Regulation's implementation. It has resulted in a proliferation of regulators with varying degrees of independence and expertise. This multiplicity creates a real risk of inconsistent interpretation and enforcement across the EU, as well as the issuance of divergent national guidance. Although Member States are encouraged to consider the advice of the European AI Board (**"AIB"**) and the Commission, there is no binding requirement to follow centralised interpretations. The result is a patchwork of national rules that undermines the AIA's core objective: the creation of a harmonised and predictable regulatory environment for

AI across the EU. For businesses, especially those operating in multiple jurisdictions, this fragmentation leads to significant legal uncertainty, increased compliance costs, and substantial barriers to innovation and market entry.

Administrative Burden and the Absence of Cross-Border Enforcement Mechanisms

A further critical weakness in the current governance regime is the lack of an effective cross-border enforcement mechanism. Unlike previous EU regulatory strategies, such as the "country-of-origin" principle, the AIA does not provide a streamlined process for addressing incidents that span multiple Member States. As a result, companies may be required to notify and interact with over 130 different authorities in the event of an incident, leading to excessive administrative burdens and operational inefficiencies. This fragmented approach not only stifles the ability of organisations to leverage AI technologies effectively but also impedes the development of a truly integrated DSM. Without a streamlined and harmonised enforcement mechanism, the EU risks falling short of its ambition to be a global leader in AI innovation and deployment.

However, by only adding a cross-border mechanism to the AIA, this would not solve this critical issue as the proliferation of regulators makes effective coordination impossible. It creates a source of conflicting interpretations and bureaucratic inefficiencies that hinder unified action and clarity for the operators. Attempting to solve these issues by new intra-regulatory cooperation mechanisms will never address the root problem - instead, it adds additional issues, including administrative burdens, further diluting accountability and absence of legal certainty.

The Missing Mandate for Innovation in Regulatory Oversight

A significant shortcoming is the lack of a clear and explicit mandate for innovation within the remit of any digital regulator, including national competent authorities. While Article 1 of the AIA emphasises the importance of fostering the adoption of human-centric and trustworthy AI, this objective is not sufficiently embedded in the mandates or competency requirements of regulatory authorities. The absence of a dedicated innovation mandate risks diluting the AIA's impact, as some authorities may interpret the promotion of innovation as a core responsibility, while others may disregard it entirely. This inconsistency not only undermines the effective implementation of the Regulation but also exacerbates regulatory fragmentation, ultimately hindering the EU's ability to compete globally in the development and deployment of cutting-edge AI technologies. Digital regulators should be aligned in their mission to create a stable environment that fosters EU goals in terms of investment, innovation, and sustainable development.

Meta

1.3.2 Complexity and Overlap in EU-Level Governance Structures

At the European level, the AIA introduces a complex and multi-layered governance framework, marked by the establishment of numerous advisory and expert groups. Each of these bodies is tasked with providing input on the implementation, interpretation, and enforcement of the Regulation. While the intention is to ensure access to specialised expertise and robust oversight, the resulting structure is highly fragmented, with overlapping mandates and ambiguous lines of responsibility. This complexity creates significant challenges for regulated entities, as the proliferation of advisory groups - each issuing guidance and recommendations, sometimes in contradiction or duplication - makes it exceedingly difficult for companies to discern which guidance is authoritative and how to prioritise their compliance efforts. The operational implications for industry are profound: the current governance model undermines the AIA's core objectives by failing to provide the clarity, predictability, and efficiency that are essential for effective oversight, compliance and innovation incentives.

1.3.3 Recommendations

- **The Need for a Unified and Efficient Mechanism for Reducing the Number of National AI Enforcers:** To ensure the AIA delivers on its promise of fostering a dynamic, innovative, and trustworthy AI ecosystem in Europe, it is essential to fundamentally reform and streamline the governance framework at both the Member State and EU levels. The regulatory architecture should be revisited to introduce a unified and efficient mechanism for reducing the number of national AI enforcers and for resolving cross-border cases. Establishing a single, primary point of contact for organisations would significantly simplify compliance and enforcement, reduce administrative burdens, and enhance legal certainty for all stakeholders. A streamlined, harmonised, and innovation-driven governance regime is indispensable for the success of the AIA. Only through decisive reform can the EU create a regulatory environment that is both protective and enabling - one that positions Europe as a global leader in trustworthy, cutting-edge AI.
- **Inclusion of Innovation in Digital Regulators' Mandate:** Equally important is the explicit inclusion of innovation as a core objective within the mandate of all digital regulatory authorities. The forthcoming Omnibus review presents a critical opportunity to enshrine this mandate in the AIA, ensuring that all digital regulators are empowered and held accountable to actively support and accelerate technological advancement. By embedding innovation at the heart of the regulatory framework, the EU can strike a vital balance between protecting individuals and enabling the responsible growth of its digital economy. By addressing the current shortcomings in governance, the EU can ensure that the AIA protects all fundamental rights by unleashing the full potential of AI to drive economic growth, competitiveness, and societal progress across the continent.

1.4 Clarify Batteries Requirements

1.4.1 Misaligned Objectives and an Impossible Timeline

The current Article 11 implementation timeline under the Batteries Regulation is unworkable and inconsistent with the EU's Better Regulation agenda. While well-intentioned, Article 11 also risks undermining Circular Economy and Ecodesign objectives for AI wearables.

Europe has long been recognised as a first-mover and global leader in the field of AI wearables. European engineers have pioneered advances in power management and thermal engineering, enabling smartglasses to deliver intensive AI capabilities - such as high-resolution displays and real-time inference - while maintaining all-day battery life. This technical edge, combined with Europe's world-renowned reputation for elegant design and user comfort, has positioned European products at the forefront of the global market. However, Article 11 risks undermining Europe's hard-won advantages. The requirement may seem reasonable for household appliances, but it is fundamentally misaligned with the realities of miniaturised, sophisticated devices like AI wearables. These products rely on custom lithium-ion chemistries and integrated thermal management systems to achieve both performance and comfort in a sleek, lightweight form factor. Forcing manufacturers to redesign devices for user-replaceable batteries would compromise the very attributes that make European technology distinctive: slim profiles, seamless integration, and safe, reliable operation. Forcing removability also raises safety risks and burdens consumers, while sealed designs are safer and more durable. While well-intentioned in principle, Article 11 risks producing outcomes contrary to the Circular Economy and Ecodesign principles and objectives. Mandating consumer-removable batteries in these devices results in weaker, shorter-lived batteries, excess expired inventory, and increased electronic waste.

Even with derogations by 2026, manufacturers would have less than one product cycle to adapt before rules apply in February 2027—a regulatory cliff edge that creates legal uncertainty and risks freezing investment in next-generation technologies.

1.4.2 Recommendation

- **Delay and Amend Article 11:** Exempt AI wearables or allow delegated acts for exemptions, aligning with Better Regulation and Competitiveness Compass goals.

2. EU Data Protection and Privacy Framework: Empowering the EU through a Modernised and Innovation-Driven Framework

The EU's data protection and privacy framework, including the GDPR and ePD are two cornerstone frameworks in the EU that impact the development of the digital economy and society. However, rapid technological change and the rise of data-driven innovation have exposed significant shortcomings in this regulatory framework. In a speech on the one-year anniversary of his landmark report on European competitiveness, delivered on September 16, at a conference hosted by Commission President Ursula von der Leyen, Draghi called not only for a pause on the "high risk" section of the AIA, but also for "radical simplification" of the GDPR.

The current regulatory approach - marked by consent absolutism, lack of proportionality, and poor consistent application with other EU digital laws - creates a complex and unpredictable environment that stifles investment and innovation. Draghi quoted research underlining that "GDPR has raised the cost of data by about 20% for EU firms compared with US peers. Yet the only change on the table so far is an easing of record keeping and extending SME derogations to mid-caps. Broader reform toward simpler, harmonised rules is still vague."

To enable the EU's leadership in digital innovation, a fundamental recalibration is needed. The data protection framework must restore balance between data protection and all the other fundamental rights and freedoms, embed proportionality and risk-based principles, and deliver legal certainty and harmonised interpretation and enforcement across the DSM. Only by addressing these structural issues can the EU unlock the full potential of its digital economy and foster responsible innovation.

Before addressing distinguishing issues regarding GDPR and the ePD, it should be noted that both pieces of legislation are strongly related. The GDPR is a *lex generalis*, on which the ePD builds as a *lex specialis*. However, the interplay between the GDPR and ePD currently generates legal uncertainty, excessive compliance burdens, inconsistency with other digital laws and regulatory fragmentation.

A major source of complexity is the ePD's over-reliance on consent, leading to a proliferation of consent requests, user fatigue, and operational uncertainty that hinders the development of the Internet of Things (**"IoT"**) and the Data Act's goals, prevents safety and integrity data uses and PETs, and creates distrust in the technology. The ePD lacks a one-stop-shop (**"OSS"**) and is supervised by regulators of different nature in each Member State. Fragmented national supervision, divergent interpretation, and inconsistent enforcement further exacerbate the lack of harmonised standards across the EU. The ePD was conceptualised when "electronic communications" were a novelty and has, since then, become outdated. If there is any merit in keeping the "electronic communications" specificity, the alignment between the two

frameworks - and their supervision and enforcement - is critical.

Addressing both instruments together is essential to ensure consistency, proportionality, and a risk-based approach across the digital regulatory landscape, as well as coherent supervision and enforcement. Isolated reform risks perpetuating legal uncertainty and regulatory fragmentation, undermining the objectives of both frameworks.

2.1 The Need to Amend the EU Data Protection and Privacy Framework

2.1.1 Proportionality, Balance, and Risk-Based Approach

The GDPR is often interpreted and enforced in a manner that elevates data protection to an absolute right, at the expense of other fundamental rights such as freedom to conduct business, freedom of expression and information, and the right to innovate. The absence of a systematic risk-based approach has fostered a zero-risk mentality, resulting in disproportionate compliance obligations and a chilling effect on data-driven innovation. This lack of balance explains why the GDPR has failed in achieving its original goals: citizens have not gained greater understanding or trust regarding data usage or technology. GDPR concepts are interpreted in such an absolutist manner that even low-risk processing activities become unnecessarily burdensome; and privacy profiteers have duly exploited these extreme positions, while competitiveness is disregarded and the market economy challenged. At a time when the EU seeks to harness its own data to drive growth in the digital and AI economy, the GDPR's unbalanced and fragmented interpretations have made personal data a "toxic" asset, making the minimisation of personal data's existence an end in itself.

2.1.2 Recommendations

- **Amend Article 1**: Explicitly include innovation and economic interests as objectives, alongside data protection. This would ensure that data protection is not interpreted in isolation, but as part of a broader framework that considers the dynamic needs of the digital economy and society.
- **Move Recital 4 (balancing rights) into Article 1**: Make the duty to balance fundamental rights arising from the Charter an explicit core principle in the GDPR. This would provide a clear legal basis for regulators and courts to weigh data protection against other rights, such as freedom to conduct a business, and would help prevent absolutist interpretations.
- **Make explicit the risk-based approach in Article 5:** Ensure proportionality and practicality in compliance. This would require that all obligations and enforcement actions be tailored to the actual risks posed by data processing, rather than applying a one-size-fits-all standard.
- **Clarify DPA mandates (Article 51 GDPR):** Require consideration of innovation and economic interests in enforcement. DPAs should be tasked with promoting a balanced

approach that supports both data protection and economic growth, and should be held accountable for ensuring proportionality in their decisions, as it is the case in any enforcement of a fundamental right or freedom.

2.1.3 Excessive Compliance Burden and Documentation

The GDPR and ePD impose extensive documentation requirements (privacy and cookies policies, risk assessments, data protection impact assessments (**"DPIAs"**)), which add additional burdensome hurdles for low-risk processing activities. These requirements are symptoms of deeper structural issues, including a lack of proportionality and a failure to distinguish between high- and low-risk processing. The result is a compliance culture focused on paperwork just created to ease regulators' work. DPA's often measure their success in the volume of fines that make headlines rather than in compliance metrics that prove substantive privacy outcomes that benefit data subjects, controllers and the society, diverting resources from innovation and growth. The current approach also fails to provide clear, practical guidance on what constitutes "manifestly unfounded or excessive" data subject requests, leading to abuse of data subject rights by privacy profiteers and increased administrative burden. The lack of scalable solutions for handling rights at scale further exacerbates the compliance burden, particularly for organizations with large user bases or complex data processing operations.

2.1.4 Recommendations

- **Systematically reduce compliance burdens:** Embed proportionality and risk-based approaches throughout the GDPR. Obligations should be scaled according to the actual risks posed by processing activities, with lighter requirements for low-risk processing.
- **Limit user-facing information requirements**: The threshold for requiring a DPIA should be clarified and raised, and organizations should be allowed to rely on sectoral codes of practice or product/processes certification schemes as evidence of compliance.
- **Provide clear, practical guidance on what constitutes "manifestly unfounded or excessive" data subject requests:** Allow scalable solutions (e.g., privacy dashboards, automated tools) for handling rights at scale and avoid fictional mandates and other proven ways to abuse Art. 80(2) by "representative organisations". This would help prevent abuse of law by data subjects and "representative organisations" and reduce the administrative burden on organisations, regulators and courts.
- **Encourage the use of standardised, user-friendly privacy notices and templates:** Rather than requiring bespoke documentation detailing every processing activity to ease regulators' work at the expense of a clear understanding of meaningful information for the citizens.

2.1.5 Fragmented, Extreme and Inconsistent Enforcement

Supervision by 40+ DPAs, divergent national laws, and the lack of a true OSS mechanism respecting the right of defense of the parties under investigation have resulted in inconsistent

rules, regulatory competition, unfair sanctions, less performant products, services or research and legal uncertainty. The European Data Protection Board's (**"EDPBs"**) intergovernmental and unaccountable structure does not enable it to deliver timely, consistent, predictable outcomes; and the current enforcement regime is slow, unpredictable, and often extreme in its outcomes. This absolutism, fragmentation and legal uncertainty undermines the single market, creates barriers to cross-border operations, and discourages investment in the EU.

2.1.6 Recommendations

- **Establish a centralised EU body**, with legal services and able to factor EU economic goals, to interpret the GDPR and ePD and issue guidance, ensuring consistency and accountability (with direct CJEU oversight). This body should be the one empowered to to issue authoritative interpretations.
- **Harmonise enforcement across GDPR, ePD, and other digital laws**, including unified breach reporting and a single lead authority for cross-border cases. Organisations should be able to interact with one regulator for all EU-wide processing activities, reducing complexity and legal risk.
- **Avoid codifying current enforcement shortcomings** as it was done in the GDPR Procedural Rules Regulation. Instead, procedural rules should be designed to promote efficiency, transparency, and predictability, protection of the right of defense of the investigated parties, with clear timelines and accountability mechanisms and avoid privacy profiteers to exploit the law.
- **Promote open stakeholder input and transparent decision-making** in the development of guidance and enforcement priorities, subject to the following principles that are applicable in other jurisdictions:
    - Consultations must occur while proposals are still at a formative stage.
    - Sufficient information needs to be supplied for the public to give the consultation 'intelligent consideration'.
    - There needs to be an adequate time for the consultees to consider the proposal and respond.
    - The product of consultation must be conscientiously taken into account when finalising the decision.

2.2 Proposed Amendments: Towards a Proportionate and Future-Proof Approach on ePrivacy

The GDPR and the ePD are interpreted and enforced in a manner that elevates data protection and privacy to absolute rights, at the expense of other fundamental rights such as freedom to conduct a business, freedom of expression and information. This also includes other key considerations such as the EU policy and legislative goals, that include the legitimate and public interests - where innovation is a driving force - in ensuring economic growth, jobs creation,

competitiveness and societal progress.

This has created a false dichotomy between the innovation and fundamental rights, as two different or even contradictory terms. To the contrary, innovation acts as a powerful enabler for fundamental rights by providing new tools, technologies, and frameworks that make these rights accessible, actionable, and meaningful in modern society. For example, advances in digital communication empower freedom of expression and access to information, while innovations in encryption and cybersecurity protect our safety as well as our privacy. Technological progress can also help bridge social and economic divides, in terms of improved access to education, healthcare, and participation in democratic processes. By continuously evolving to address emerging challenges and opportunities, innovation not only supports the realisation of fundamental rights but also adapts them to the changing needs of individuals and communities in a digital age.

The ePD compounds these issues by imposing outdated, overlapping, and redundant requirements - most notably through its consent-only regime for cookies and traffic data. This approach is incoherent with the GDPR and other digital laws, is contrary to the ambitions of the Data Act, and is incompatible with the realities of the modern digital economy, including AI and IoT development. The lack of explicit recognition of economic interests and innovation as objectives for regulators has led to a regulatory culture that is risk-averse, data-averse, and inflexible, undermining the EU's digital competitiveness, which is based on infrastructure, technology, data and expert human capital.

2.2.1 Consent Absolutism and Legal Bases

The current interpretation of the data protection and privacy frameworks fosters a "consent absolutism" culture, particularly in the ePD's cookie and traffic data rules. This has resulted in widespread banner fatigue, user desensitisation, and operational inefficiency as well as technology distrust, without delivering meaningful privacy protection or digital literacy regarding the important role cookies play in the internet ecosystem. The misconception that consent is the preferred, more protective or superior legal basis for processing personal data has led to over-reliance on consent, even where other legal bases (such as legitimate interest) would be sometimes more appropriate and less burdensome. Often, legitimate interest can provide more protection due to the importance of safeguards as part of the legitimate interest balancing exercise. On the contrary, if controllers simply manage to obtain consent (or not) they are not incentivised to implement additional mitigations, or they are just unable to run a business activity in a stable manner. This consent-based regime hinders the development of the IoT that other digital laws are looking for, as part of the EU DSM.

Furthermore, the over-reliance on consent is highly problematic for low-risk processing activities or whether other interests must be balanced against, such as analytics, measurement, safety and integrity activities. This includes the prevention and detection of

fraud or other criminal activities, the use ofPETs, or the use of data gathered by cookies for purposes relying on GDPR legal basis other than consent.

The emphasis on consent also undermines user experience, as individuals are confronted with frequent and often meaningless consent requests, leading to "consent fatigue" and reduced trust in digital services. This leads to less accountability of both controllers and DPAs, since citizens bear the burden to decide on whether to agree with numerous daily routine digital activities with distrust and resignation. Furthermore, the lack of harmonisation in the interpretation and enforcement of ePD definitions and consent requirements across Member States, and the misuse of ePD to overcome the GDPR OSS, creates further legal uncertainty and operational complexity for businesses operating in multiple jurisdictions.

2.2.2 Recommendations

- **Modernise cookie rules** by either disapplying ePD 5(3), or incorporating all GDPR legal bases for cookies and similar technologies. This would allow organisations to rely on legitimate interest or contractual necessity, rather than being forced to obtain consent for every use of cookies, and would reduce banner fatigue for users.
- **Create consent exemptions for low-risk use cases**, such as analytics or measurement, legitimate activities protecting safety and integrity (including fraud/crime prevention and detection) and contractual compliance, employment-related data as well as purposes of use that rely on a GDPR legal basis other than consent. These exemptions should be clearly defined and harmonised across the EU, drawing on best practices such as the UK Data Protection and Digital Information Bill.
- **Recognise PETs as a basis for exemption from consent requirements**. Where PETs are used to minimise or eliminate the collection of personal data, or to generate synthetic or aggregated datasets, consent should not be required.
- **Align traffic data provisions with GDPR**, allowing legitimate interest and public interest as legal bases. This would enable innovation in connected vehicles, IoT, and safety-critical services, while maintaining appropriate safeguards for user privacy.
- **Clarify that all GDPR legal bases are equally valid** and appropriate depending on context. Guidance should explicitly remind that there is no hierarchy among legal bases, and that organisations are free to choose the most appropriate basis for their processing activities.

2.2.3 Outdated and Redundant ePrivacy Rules

The ePD's cookie and traffic data provisions are misaligned with the GDPR and modern digital realities, creating legal uncertainty and stifling IoT and AI development. The direct marketing by electronic communications regime is outdated, inconsistently implemented, contrary to GDPR and inconsistent with CJEU requirements. The fragmented enforcement landscape, where either both DPAs or telecom regulators are involved depending on the Member State and

without any OSS mechanism or country-of-origin principle, further complicates compliance and increases costs. The ePD's approach to cookies and traffic data is particularly problematic, as it fails to recognise the essential role of these technologies in the functioning of the digital economy and the development of PETs. The lack of harmonisation in the interpretation and enforcement of ePD provisions across Member States creates further legal uncertainty and operational complexity for businesses.

2.2.4 Recommendations

- **Remove or align outdated ePD provisions** (cookies, traffic data, direct marketing) with the GDPR and the Data Act. The ePD should be repealed or fundamentally revised to
    - Eliminate duplication,
    - Ensure consistency with the GDPR's risk-based approach and legal basis.
- **Repeal or significantly amend the ePD's direct marketing regime** to make it compatible with GDPR, including its Recital 47. The GDPR was adopted for the Internet era and therefore the fact that direct marketing is conducted by electronic means does not require a different regulation. It should be regulated only under the GDPR, with clear rules on the use of legitimate interest and objection rights, and harmonised across Member States.
- **Empower the Commission to adopt delegated acts for future-proofing**. The regulatory framework should be flexible enough to adapt to new technologies and business models, with the Commission able to introduce exemptions or clarifications as needed.
- **Harmonise enforcement with centralised interpretation and unified breach reporting**. Organisations should only be required to report serious breaches to a single lead authority, covering GDPR, ePD, and the European Electronic Communications Code (**"EECC"**).

2.2.5 Fragmented and Inconsistent Enforcement

The ePD's fragmented interpretation and implementation across Member States has led to inconsistent interpretations, enforcement gaps, and significant legal uncertainty. This is not only linked to the fact that the regulators are multiple and of different profiles but also because there is no effective coordination/consistency mechanism among them. The ePD forces companies to navigate a patchwork of regulators and inconsistent rules, which is particularly notable in the case of the data protection regulators. This fragmentation and often absolutist approach by data protection regulators (which are not the unique enforcers of the ePD national implementation) increases compliance costs and complexity, undermines trust in enforcement, and creates barriers to innovation, the development of the IoT pursued by the Data Act.

2.2.6 Recommendations

- **Establish a centralised EU body to interpret the ePD**, issue guidance, be transparent in its actions, ensure consistency and accountability (with direct CJEU oversight),

respecting the right of defense, factoring the EU economic and policy goals in its decision-making processes and truly incorporating effective public consultation principles.

- **Introduce a unified data breach reporting model**, so that data breaches are reported only if they are serious and to one 'lead authority' for ePD, EECC and GDPR.

2.2.7 Conflicts with Other EU Digital Laws

Overlapping and contradictory requirements with the AIA, the Data Act, DGA, DSA, DMA, and NIS2 Directive, impede the objectives of the EU Digital Strategy. The lack of clarity on the relationship between these laws and the GDPR/ePD creates legal uncertainty and operational risk, particularly in areas such as transparency, data minimisation, legal basis (consent or otherwise), anonymisation and special categories of data. This is especially problematic for AI and data-driven services, which rely on large, diverse datasets and flexible data processing rules. The cross-referencing of GDPR concepts in other digital laws, such as the use of GDPR consent in the DMA, often results in the inappropriate application of standards created for different policy objectives and tools, undermining the effectiveness of these laws, the required legal certainty for businesses and the citizens' trust in the digital economy.

2.2.8 Recommendations

- **Fully align ePD Articles 5, 6, and 13 with the GDPR**, recognising all GDPR legal bases and ensuring proportionality.
- **Clarify the relationship of the GDPR and ePD with other digital laws**, particularly regarding transparency, proportionality (data minimisation), legal basis, anonymisation or special categories of data. Guidance should specify if and, if so, how these principles apply in the context of the AIA, Data Act, DGA, DSA, DMA, and NIS2 Directive, taking into account the respective and different policy and legislative objectives.

3. Cybersecurity Reporting: A Call for Harmonisation and Simplification

While vital EU instruments like the NIS2 Directive are establishing a high common level of cybersecurity, their ultimate effectiveness is being undermined by fragmented and duplicative implementation at the Member State level. The current patchwork of national compliance and reporting obligations creates significant administrative burdens, legal uncertainty, and compliance friction, particularly for businesses operating across borders. This fragmentation forces companies to navigate a mosaic of different portals, templates, languages, and timelines for a single cross-border incident.

The lack of a harmonised and centralised model creates an environment where critical resources are diverted from incident mitigation to administrative paperwork, a reality that directly conflicts with the EU's goals to promote simplification and harmonisation of EU

regulatory frameworks. Put simply, the current trajectory risks undermining security by focusing on procedural compliance over substantive outcomes.

A fundamental recalibration is necessary. Simplifying the regulatory framework through targeted harmonisation is not merely an administrative exercise; it is an essential strategic imperative for enhancing the EU's collective cybersecurity resilience, reducing friction in the DSM, and ultimately, securing the Union's digital sovereignty.

3.1 Proposed Solutions for Simplification and Harmonisation

We have set out concrete, actionable proposals for the Commission, grounded in direct operational experience and drawing upon proven models from existing EU frameworks, including the reporting arrangements for the GDPR. These solutions are designed to decisively reduce the administrative burden on businesses while simultaneously improving the speed, quality, and consistency of incident reporting and cross-border supervisory cooperation.

3.1.1 Fragmented and Duplicative Reporting Obligations

The most immediate and burdensome challenge for operators is the fragmented nature of incident reporting itself, where a single cybersecurity event can trigger numerous, inconsistent, and overlapping reporting obligations across the EU.

Issues

- **Multiple, Overlapping Reporting Requirements:** A single cross-border security incident can trigger separate reporting obligations under NIS2, GDPR, the EECC, and sectoral rules, each with different thresholds, timelines, and content requirements. This results in parallel and duplicative submissions to multiple national authorities.
- **Divergent National Portals and Templates:** Operators must navigate a complex patchwork of national reporting portals and templates that vary significantly in language, required data fields, and evidence expectations. This fragmentation increases internal coordination costs and slows down incident response.
- **Divergent Significance Thresholds and Definitions:** Inconsistent definitions and thresholds for what constitutes a "significant" incident across Member States and legislative frameworks create legal uncertainty and can lead to both over-reporting and ambiguity.
- **Operational Inefficiency:** The cumulative effect is a staggering drain on resources, diverting attention from critical incident mitigation to burdensome paperwork. A single cross-border incident can require operators to submit up to 108 reports, with a minimum of 81 separate notifications and responses to follow-up requests, turning an operational crisis into an administrative one.

Recommendations

- **Establish an EU-level, single reporting portal hosted by the European Union Agency for Cybersecurity ("ENISA")**. This portal should feature secure access for entities and authorities, unified forms (for early warnings, notifications, and final reports), automated distribution to all relevant national authorities, and support for machine-readable formats and APIs to enable automation.
- **Allow reporting in a single common language** to eliminate the significant administrative burden and delays associated with translating reports for multiple jurisdictions.
- **Mandate harmonised EU templates for incident reporting** and establish a "single mailing list/central distribution" mechanism to allow one submission, by way of a one-time email or central distribution-portal, to reach all competent authorities simultaneously.

However, a streamlined portal is only as effective as the rules it enforces. To achieve true simplification and move beyond procedural fixes, the substantive legal and regulatory requirements must be harmonised.

3.1.2 Excessive Compliance Burdens and Lack of Proportionality

The compliance burden extends beyond incident reporting to include overlapping risk management requirements and a lack of mutual recognition between frameworks. This leads to redundant work and a disproportionate focus on documentation over substantive security outcomes.

Issues

- **Overlapping Risk-Management Requirements:** Key legislation such as the NIS2 Directive, the Cyber Resilience Act (**"CRA"**), the Digital Operational Resilience Act (**"DORA"**), and sectoral rules impose similar yet distinct risk-management requirements without providing a clear mapping or a presumption of conformity between them, leading to redundant controls.
- **Lack of Mutual Recognition:** The absence of "deeming" clauses or mutual recognition means that a compliant report or audit in one Member State does not satisfy the requirements in another, even when the substance is nearly identical. This forces organizations to undergo redundant audits and answer duplicative follow-up requests.
- **Focus on Documentation over Outcomes:** The combination of these burdens results in excessive documentation, repetitive audits, and a compliance culture focused on paperwork rather than on achieving tangible improvements in security posture.

Recommendations

- **Create a unified rulebook for incident reporting** that harmonises key definitions (e.g., "significant/severe"), reporting thresholds, and timelines across NIS2 Directive, the CRA, and DORA.
- **Implement mutual recognition and "deeming" clauses** so that a single compliant report submitted for an incident can satisfy multiple legislative obligations where the scope and substance of the incident align.
- **Publish a unified set of risk-management requirements** or, alternatively, develop a "cross-walk and presumption-of-conformity" approach that maps requirements across NIS2, the CRA, DORA, and sectoral rules to eliminate redundant controls.
- **Allow for the acceptance of credible external attestations and certifications** as evidence of compliance to reduce the need for repetitive internal and external audits.

With aligned rules and proportional requirements in place, the final critical element is a clear and coordinated governance structure to ensure these harmonized processes are managed effectively at the EU level.

3.1.3 Absence of a Coordinated EU Governance Model

A harmonised system requires a clear and consistent governance model to function effectively. Lessons from successful EU frameworks demonstrate the feasibility and efficiency of a more coordinated approach to supervision and reporting.

Issues

- **The absence of a central coordinating body** for incident reporting places the entire burden of multi-authority communication and distribution on the reporting entity, increasing complexity and the risk of error.
- **The current cybersecurity framework lacks a single, predictable point of contact** for cross-border incidents, which leads to inconsistent supervisory engagement and follow-up across Member States.
- **There is ambiguity regarding the precise operational role ENISA** should play in facilitating a harmonised system, which requires clear definition to ensure accountability and effectiveness.

Recommendations

- **The model should draw on precedents from the EU's own regulatory toolkit:** DORA's successful creation of a single, streamlined framework; the GDPR's one-stop-shop; and the EECC/BEREC's use of template governance, which demonstrates how to harmonize national practices effectively.
- **The role of ENISA should be clearly defined as the coordinator** for the single portal's technical design, templates, maintenance, and distribution rules. ENISA should provide guidance and best practices but should not become a conformity assessment body or market surveillance authority.
- **Member States would retain their full supervisory and enforcement powers.** The centralised system would benefit them by ensuring they receive more timely, complete, and consistent information, thereby enhancing their ability to protect citizens and critical infrastructure.