Response to the European Commission's Digital Fitness Check Consultation

Moving beyond surface-level simplification of the EU digital rulebook

March 2026

The Computer & Communications Industry Association (CCIA Europe) welcomes the European Commission's Digital Fitness Check as an opportunity to address the fundamental simplification needs of the EU digital rulebook – going beyond the limited scope of the Digital and AI Omnibus proposals. CCIA Europe offers the following 18 recommendations.

I. Eliminating duplication across different rules

The EU rulebook currently mandates duplicative, overlapping compliance processes for identical risks across laws. Consolidation is essential to reduce administrative overhead.

Recommendations:

1. AI & data governance – Mutually recognise firms' overlapping impact assessments
2. Data governance – Establish a unified approach to automated decision-making
3. Cybersecurity – Create a single, standardised reporting framework
4. Content moderation – Eliminate duplicative TCO & CSAM regimes
5. Data governance – Guarantee consumers' right to transfer their own data

II. Streamlining compliance within specific laws

The European Commission should actively tackle instances where a single piece of legislation is procedurally broken, overly broad, or redundant on its own.

Recommendations:

6. Data governance – Fix Data Act's overbroad scope and remove commercial barriers
7. Platform economy – Confirm repeal of the Platform-to-Business Regulation
8. Content moderation – Rationalise DSA transparency reporting obligations
9. Market contestability – Improve DMA enforcement's predictability and procedures

III. Resolving direct legal frictions & sectoral creep

Conflicting mandates across different EU laws place businesses in legal deadlocks. Clear hierarchies are needed to restore certainty for digital services and the wider ecosystem.

Recommendations:

10. Data protection – Resolve the GDPR and ePrivacy dual-consent deadlock
11. Content moderation – Halt sectoral creep undermining the DSA's monitoring ban
12. Media – Reconcile conflicting DSA & EMFA content-moderation mandates
13. E-Commerce – Ensure alignment between the DSA and other sectoral rules
14. Intellectual property – Prevent automatic injunctions and ensure FRAND licensing

IV. Strengthening governance & future rulemaking

The long-term success of the digital rulebook depends on unified enforcement mechanisms, regulatory cooperation, and a strict commitment to evidence-based policymaking.

Recommendations:

15. Governance – Implement the AI Act proportionately, moratorium on new regulation
16. Single Market – Ensure 'one-stop-shop' and 'country of origin' across borders
17. Cooperation – Establish baseline enforcement rules for regulatory authorities
18. Better regulation – Mandate impact assessments for late-stage legislative changes

Introduction

The Computer & Communications Industry Association (CCIA Europe) applauds the European Commission's consultation on the upcoming Digital Fitness Check. As highlighted in the Draghi and Letta reports, overlapping digital regulations impose disproportionate compliance costs on companies operating across the European Union. This regulatory overlap contributes to what the IMF describes as a "110% tariff"[1] on cross-border services within the EU, also hindering the bloc's global competitiveness.

CCIA Europe commends the Commission for kicking off a much-needed discussion on broader simplification of the EU digital rulebook – moving beyond the limited tweaks of the recent AI and Digital Omnibus proposals. Meaningful simplification, however, requires a fundamental restructuring of the digital acquis to make EU laws more coherent, predictable, and grounded in operational realities. To untangle today's compliance deadlocks, CCIA Europe's offers 18 recommendations, structured around four imperatives:

I. Eliminating duplication across different rules
II. Streamlining compliance within specific laws
III. Resolving direct legal frictions and sectoral creep
IV. Strengthening governance and future rulemaking

These imperatives span the full digital acquis – from data governance and ePrivacy to content moderation, AI, and platform regulation — and are grounded in the political mandate set out in the Draghi and Letta reports,[2] the European Commission's Competitiveness Compass,[3] as well as specific legislative reviews such as the Commission's own Article 33 review of the Digital Services Act.[4]

[1] Regional Economic Outlook: Europe; A recovery short of Europe's full potential, IMF, October 2024: https://www.imf.org/en/publications/reo/eu/issues/2024/10/24/regional-economic-outlook-europe-october-2024

[2] The Draghi report: A competitiveness strategy for Europe, 2024; Much More Than A Market, Enrico Letta's Report on the Future of the Single Market, 2024.

[3] A Competitiveness Compass for the EU, Communication, January 2025, https://commission.europa.eu/topics/competitiveness/competitiveness-compass_en

[4] Report on application of Article 33 of Regulation (EU) 2022/2065 (DSA) and the interaction of that Regulation with other legal acts, and Staff Working Document on the application of Article 33 of Regulation 2022 2065 and the interaction of that Regulation with other legal acts, 17 November 2025, available at https://digital-strategy.ec.europa.eu/en/library/report-application-article-33-regulation-eu-20222065-dsa-and-interaction-regulation-other-legal

A simpler, more consistent digital rulebook is the strategic lever Europe needs to drive innovation, ease cross-border operations, and safeguard its position in the global market. Crucially, it will also ensure that EU companies and merchants of all sizes can continue to leverage digital platforms, commerce infrastructure, and cloud-based tools to reach customers across borders without facing fragmented or contradictory regulatory requirements.

I. Eliminating duplication across different rules

The EU rulebook currently mandates duplicative, overlapping compliance processes for identical risks across laws. Consolidation is essential to reduce administrative overhead.

1. AI & data governance – Mutually recognise firms' overlapping impact assessments

EU digital legislation currently imposes overlapping impact assessment requirements on companies operating the same systems. A single automated decision-making system – whether used for a digital labour platform, B2B fraud prevention, merchant onboarding, or trust and safety processes – may simultaneously trigger a Data Protection Impact Assessment (DPAI) under the General Data Protection Regulation (GDPR), a Fundamental Rights Impact Assessment under the AI Act, and reporting obligations under the Platform Work Directive – each with distinct methodologies, yet assessing substantially similar risks. The Digital Omnibus proposal tries to address DPIA duplication but leaves this broader coordination gap unresolved. The result is compounded compliance burden without commensurate benefit to the individuals these frameworks are designed to protect.

The Commission should operationalise an 'assess-once-comply-many' approach by introducing an explicit mutual recognition clause enabling reuse of assessment outputs across the GDPR, AI Act, and the Platform Work Directive. Given that these frameworks already rely on comparable risk-based methodologies for automated processing, common templates could establish a shared baseline – covering risk analysis, system descriptions, and safeguards – while accommodating regime-specific additions where necessary. This would eliminate unnecessary duplication, improve consistency across EU digital legislation, and support proportionate compliance (without lowering protection standards or constraining regulatory discretion).

Call to action: The Commission should clarify, within the Digital Omnibus package or a dedicated coordination instrument, that a **comprehensive DPIA under GDPR satisfies equivalent requirements under the AI Act and Platform Work Directive where the underlying risks and systems are equivalent**. To operationalise this, the Commission should mandate the development of interoperable assessment templates companies can reuse across all relevant regulatory frameworks to drastically reduce administrative burdens.

2. Data governance – Establish a unified approach to automated decision-making

The EU regulatory framework features at least three separate and mutually inconsistent approaches to automated decision-making (ADM), with no binding mechanism to resolve their interaction.

Article 22 of the GDPR adopts a decision-centric approach, restricting "automated individual decision-making" that produces legal or similarly significant effects on a data subject. Yet, the threshold for what qualifies as "similarly significant" remains undefined, leading to divergent national interpretations. This ambiguity risks sweeping in routine digital tools used by businesses to personalise services, detect fraud, allocate resources, or improve customer experience – inappropriately treating them as high-risk processing, even when they have limited impact on individual rights.

Meanwhile, the Platform Work Directive (PWD) takes a system-based approach, covering decisions that "significantly affect persons" regardless of whether the final output is fully automated or involves human review. The AI Act, meanwhile, applies a risk-based lens to the underlying system, potentially capturing a wide range of rule-based tools that fall entirely outside the scope of either the GDPR or the PWD. The result is that the same business process – driver allocation, delivery dispatch, or an automated onboarding step – may simultaneously trigger overlapping and contradictory obligations under three separate regulatory regimes, each overseen by a different supervisory authority.

This structural incoherence places businesses in a genuine compliance deadlock. Companies subject to all three frameworks face duplicative impact assessment obligations for the same systems, with no authoritative guidance on how to sequence or consolidate them. Absent a common cross-regulatory definition of ADM and a clear hierarchy governing which instrument takes precedence, companies cannot determine in good faith whether satisfying their obligations under one act creates liability under another.

The absence of a unified definition also obstructs a genuine 'assess-once-comply-many' approach to impact assessments: where the GDPR's DPIA, the AI Act's Fundamental Rights Impact Assessment, and the Platform Work Directive's reporting obligations for automated monitoring systems all address overlapping risks for the same system, requiring separate assessments under each piece of legislation delivers administrative burden without commensurate benefit to individuals.

This fragmentation extends beyond decision-making definitions to the foundational role concepts based on which each framework allocates responsibility. The GDPR assigns obligations through the controller/processor distinction (Articles 4(7) and 4(8)), while the AI Act introduces a parallel taxonomy of provider, deployer, and distributor (Article 3) – carrying separate and potentially conflicting obligations. A company deploying a third-party AI system that processes personal data may simultaneously qualify as a GDPR controller, an AI Act deployer, and potentially an AI Act provider if it fine-tunes or materially modifies that system. Each characterisation triggers its own compliance regime, with no mechanism to reconcile overlapping or contradictory obligations.

This lack of clarity is particularly acute in the context of joint controllership under the GDPR. Where a deployer integrates a third-party AI system into its operations, it remains unclear

whether this creates sole controllership, joint controllership with the AI provider, or a controller-processor relationship. Yet this determination has significant consequences for liability allocation, data subject rights, and supervisory authority jurisdiction. Without authoritative guidance, companies are left to make these characterisations unilaterally, with the risk that different national authorities reach conflicting conclusions based on the same factual case.

Call to action: The Omnibus does not resolve the broader cross-regulatory fragmentation around ADM. The Commission, in cooperation with the EDPB and relevant competent authorities, should **develop and publish binding joint guidance on the sequencing and interaction of transparency, explainability, and impact assessment obligations under the GDPR, AI Act, and the Platform Work Directive** — providing companies with authoritative clarity on how to comply coherently across all three regimes for the same system. This guidance must provide companies with absolute legal clarity on how to comply coherently across all three regimes for the same system, explicitly ensuring that low-risk, routine commercial automation tools are shielded from compliance regimes designed for high-risk use cases. Finally, this guidance should also **clarify how GDPR controller/processor concepts map onto AI Act provider/deployer roles**, including how responsibility shifts when a deployer fine-tunes or customises a third-party AI system.

3. Cybersecurity – Create a single, standardised reporting framework

While the Digital Omnibus proposal aims to establish a single technical interface to report security incidents in the EU, the underlying regulatory framework remains a patchwork of conflicting cybersecurity obligations.

Under existing laws and proposals, entities must navigate a 'triple-clock' dilemma for a single event: 24 hours for an early warning under the NIS2 Directive, 72 hours for standard practice, and 96 hours for high-risk GDPR breaches. This forces security teams to prioritise stopwatch management over active cyberthreat mitigation. In addition, significant legal uncertainty persists regarding when the reporting clock actually begins. Without a common trigger, companies are left to guess whether the countdown starts at initial detection or at formal confirmation. Furthermore, subjective terms like 'high risk' (GDPR) and 'significant incident' (NIS2) lack a shared baseline, leading to inconsistent severity assessments across different jurisdictions.

Furthermore, the 'single-entry point' portal put forward by the Digital Omnibus proposal is merely a cosmetic fix if the data behind it is not standardised. Without a single, harmonised reporting form, companies still have to manually format the same evidence for different regulators using outdated PDF reports. Without automated data sharing, security teams are forced to act as administrative translators for regulators, rather than focusing on their actual job: detecting and stopping cyber attacks.

Call to action: The Commission should **introduce a new cybersecurity Omnibus to standardise reporting timelines around a single 72-hour deadline for all regulations covered by the single-entry point** – aligning NIS2, GDPR, the Digital Operational Resilience Act (DORA), and the Cyber Resilience Act (CRA). It must ensure alignment around reporting thresholds, including **unambiguous language which explicitly starts the reporting clock when an incident is confirmed, not when merely suspected or detected**. Similarly, the new Omnibus should also include harmonisation of definitions of 'high risk'

(GDPR) and 'significant incident' (NIS2) via implementing acts to ensure consistent severity assessments.

Further simplification efforts are needed to **evolve the single-entry point into a digitally interoperable infrastructure by harmonising the reporting template and mandating a common EU-wide evidence taxonomy** across the acquis. This must include automated evidence mapping and machine-readable formats (such as OSCAL), enabling organisations to generate structured data once and reuse security documentation across compliance regimes to satisfy multiple authorities. Post legislation, EU-level guidance should be produced to ensure consistent supervision, which would reduce interpretative gaps during audits.

4. Content moderation – Eliminate duplicative TCO & CSAM regimes

The Digital Services Act (DSA) was designed to serve as the EU's definitive horizontal framework for content moderation and risk management. However, its effectiveness now risks being undermined by overlapping, content-specific instruments.

As highlighted in the Commission's own November 2025 Article 33 report on the DSA,[5] parallel regimes like the Terrorist Content Online (TCO) Regulation and the proposed Regulation to prevent and combat child sexual abuse material (CSAM Regulation) are among the most significant sources of duplication, imposing compounded compliance costs without delivering additional protections.

The TCO Regulation, adopted prior to the DSA, was designed to address a specific content category in the absence of a horizontal framework. That framework now exists. Core TCO mandates regarding removal orders, specific risk mitigation measures, transparency reporting, and complaint mechanisms (Articles 3 to 5, 7, and 10) are now substantially duplicated by the DSA's comprehensive notice-and-action (Articles 16 to 17), trusted-flagger (Article 22), and systemic-risk (Articles 34 to 35) frameworks. Maintaining both forces platforms to execute identical risk management exercises under different legal headings.

This structural duplication threatens to expand even further with the proposed CSAM Regulation, currently undergoing trilogue negotiations. As originally drafted by the Commission, it risks establishing an entirely parallel architecture for risk assessments and transparency reporting that directly mimics existing DSA obligations for Very Large Online Platforms (VLOPs). Furthermore, untargeted detection obligations under the proposed CSAM rules threaten to impose general monitoring mandates, directly conflicting with DSA Article 8's ban and established CJEU case law.[6] Forcing platforms to run parallel, duplicative reporting streams undermines vital engineering resources for trust and safety that should be focused on mitigating existing risks.

---

[5] Report on application of Article 33 of Regulation (EU) 2022/2065 (DSA) and the interaction of that Regulation with other legal acts, and Staff Working Document on the application of Article 33 of Regulation 2022 2065 and the interaction of that Regulation with other legal acts, 17 November 2025, available at https://digital-strategy.ec.europa.eu/en/library/report-application-article-33-regulation-eu-20222065-dsa-and-interaction-regulation-other-legal

[6] Judgment of the Court (Third Chamber) of 3 October 2019 (request for a preliminary ruling from the Oberster Gerichtshof – Austria) – Eva Glawischnig-Piesczek v Facebook Ireland Limited (Case C-18/18), available here: https://infocuria.curia.europa.eu/tabs/affair?sort=AFF_NUM-DESC&searchTerm=%22C-18%2F18%22&publishedId=C-18%2F18

Call to action: The Commission must **use the Digital Fitness Check to formally consolidate the EU's content moderation architecture under the DSA**. This would require repealing the redundant provisions of the TCO Regulation and integrating its substantive objectives, such as the one-hour removal requirement, into the DSA's existing frameworks for illegal content orders (Articles 9 and 10), while maintaining appropriate procedural safeguards. Furthermore, co-legislators should ensure the final CSAM Regulation explicitly recognises that a platform's compliance with the DSA's systemic-risk assessment (Article 34) and transparency reporting (Article 42) obligations fully satisfies the equivalent mandates under the CSAM framework, ensuring a single, unified compliance stream.

5. Data governance – Guarantee consumers' right to transfer their own data

The Digital Omnibus proposal misses a critical opportunity to resolve a fundamental contradiction within the EU rulebook that currently traps businesses in a compliance deadlock. Indeed, Article 5(2) of the Data Act prohibits companies designated as 'gatekeepers' under the Digital Markets Act (DMA) from acting as authorised third parties for data access – a restriction that stands in direct opposition to the user's portability rights guaranteed under Article 20 GDPR and the contestability measures of DMA Article 6(9).

This regulatory friction forces all companies holding user data into an untenable position: fulfilling a valid user request to port data to a gatekeeper violates the Data Act, while refusing that same request invites liability under the GDPR and DMA.[7]

The Commission recently suggested in a non-binding guidance[8] document that the restriction of Article 5(2) of the Data Act only applies to "mandatory" data-sharing mechanisms and leaves "voluntary arrangements" unaffected, reflecting the equally evasive and non-binding language of Recital 40.

However, neither the Commission's guidance on Article 5(2), nor Recital 40 resolve the inherent conflict. User portability rights under the GDPR and DMA are binding statutory obligations, not voluntary business arrangements. Article 5(2) contains no textual exception for user-initiated data transfers, and neither the non-binding language of a Recital nor administrative guidance can overrule the plain, unambiguous language in binding provisions of the Data Act. In other words, companies cannot defend against enforcement actions by citing non-binding language such as some Commission FAQ that contradicts the very statute they may be charged with violating.

Beyond the administrative burden, this incoherence actively undermines the EU's competitiveness agenda. By effectively blocking consumers from transferring their data to the service provider of their choice, the current framework inadvertently fosters lock-in and nullifies the individual's control over their personal data. To deliver genuine simplification and legal certainty, the Omnibus must establish a definitive hierarchy of norms. It must be

[7] See Data Act's Undue Data Portability Restrictions: CCIA Requests EU Privacy and Competition Enforcers To Step In, CCIA Europe (June 2023), https://ccianet.org/news/2023/06/data-acts-undue-data-portability-restrictions-ccia-requests-eu-privacy-and-competition-enforcers-to-step-in/

[8] See Frequently Asked Questions on the Data Act, section 36, version 1.4 (January 2026), https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act, and and last sentence of Recital 40 Data Act: "As voluntary agreements between gatekeepers and data holders remain unaffected, the limitation on granting access to gatekeepers would not exclude them from the market or prevent them from offering their services."

made clear that industrial policy restrictions in the Data Act cannot supersede the fundamental right of users to freely port their data.

Call to action: If this problem is not addressed in the Digital Omnibus, the European Commission should urgently **introduce a targeted amendment to the Data Act clarifying that the exclusion of gatekeepers in Article 5(2) of the Data Act is without prejudice to, and does not restrict, the exercise of user-initiated data portability rights** under the GDPR or the DMA.

II. Streamlining compliance within specific laws

The European Commission should actively tackle instances where a single piece of legislation is procedurally broken, overly broad, or redundant on its own.

6. Data governance – Fix Data Act's overbroad scope and remove commercial barriers

The Data Act's current scope inadvertently sweeps in entities and products it was never intended to regulate, while simultaneously creating duplicative compliance regimes.

For instance, Chapter II of the Data Act overlaps almost entirely with consumer rights already established under the GDPR, effectively penalising EU businesses with double regulation for the exact same data without providing meaningful additional protections to consumers. Furthermore, the broad definition of a 'connected product' captures general-purpose consumer electronics (like smartphones, PCs, and tablets) and highly regulated financial hardware, like point-of-sale (POS) terminals, straying far from the Act's original focus on industrial internet-of-things data.

Similarly, the sweeping definition of 'data processing services' inappropriately captures B2B Software-as-a-Service (SaaS) providers, forcing heavy-handed cloud infrastructure-switching rules onto software application layers that operate under fundamentally different technical and commercial models.

Beyond scoping errors, the legislative framework introduces artificial market barriers that disrupt standard B2B commercial practices. Most notably, the Act's broad restrictions on switching charges and contractual terms severely undermine cloud providers' ability to offer upfront discounts for long-term, fixed-term commitments. Standard B2B practices – where enterprise customers receive significant price reductions in exchange for a committed usage term – are jeopardised if providers cannot enforce proportionate early termination fees to recover those advanced discounts when a customer breaks the contract early. Adding to this friction, the Act allows public sector bodies to charge higher, discriminatory fees to very large enterprises and gatekeepers for the re-use of open government data, preventing capable actors from building valuable services and AI models on public data.

Call to action: First, **consumer data must be carved out from Chapter II of the Data Act, relying solely on the GDPR** as the single standard for consumer data rights. Second, **definitions must be narrowed: 'data processing services' must exclude B2B SaaS entities, and 'connected products' must explicitly exclude personal consumer devices**

and POS terminals. Finally, the framework must be amended to explicitly protect standard B2B discount structures by permitting proportionate early termination fees for fixed-term contracts, and it must remove discriminatory fee provisions for open government data to ensure a level playing field.

7. Platform economy – Confirm repeal of the Platform-to-Business Regulation

The Platform-to-Business (P2B) Regulation (EU) 2019/1150 was adopted to improve fairness and transparency in the relationship between online platforms and their business users. Since its entry into force, however, the regulatory landscape it was designed to address has been fundamentally reshaped by the DSA and the DMA, both of which impose far more comprehensive transparency, fairness, and complaint-handling obligations. The P2B Regulation's core requirements – from internal complaint-handling systems to transparency of ranking parameters and the obligation to publish annual effectiveness reports – are now either directly superseded by or substantively duplicated within these newer horizontal instruments.

Maintaining the P2B Regulation as a standalone instrument forces platforms into duplicative compliance exercises that generate neither meaningful oversight nor practical value for business users. The annual reporting obligation under Article 11(3), for example, has proven particularly unworkable: business users typically route complaints through general support channels rather than dedicated P2B mechanisms, producing datasets that are neither reliable nor reflective of actual dispute volumes. The resulting reports remain largely unused by regulators and the broader public.

Call to action: CCIA Europe supports the proposal included in the Digital Omnibus on the digital acquis to **repeal the P2B Regulation. With the DSA and DMA now operational, the consumer and business user-protection objectives originally pursued by the P2B Regulation are fully addressed by the current horizontal framework**. Repeal would eliminate a redundant compliance layer without any reduction in the protections available to business users.

8. Content moderation – Rationalise DSA transparency reporting obligations

The Digital Services Act's (DSA) transparency architecture imposes overlapping disclosure obligations that generate administrative cost without commensurate informational value. Under Articles 15(1), 24(1), and 42(2), online platforms and Very Large Online Platforms must compile and publish annual transparency reports covering content moderation decisions, notices received, internal complaint handling, and out-of-court dispute settlement activity. In parallel, Article 24(5) requires online platforms to upload, in near-real-time, every individual content moderation decision to the Commission's DSA Transparency Database.

This creates a structural duplication: platforms are required to report granular, decision-level data to a centralised database and then manually aggregate and re-report substantially the same information in a separate annual document. The annual report obligation further requires the disclosure of operational data that may constitute commercially sensitive information, without a clear mechanism for protecting business confidentiality. For companies operating across multiple EU Member States, the compliance burden of preparing, verifying, and publishing these overlapping reports is significant – and

the incremental value to regulators or the public is questionable where the underlying data is already available in machine-readable form via the Transparency Database.

Call to action: The Commission should **review the necessity of the annual transparency report in light of the real-time DSA Transparency Database**. Where data points are already captured in the database, the annual obligation should be limited to a narrative summary covering information not otherwise publicly available. The Commission should also assess whether commercially sensitive data reported through these channels can be shielded from public disclosure while remaining accessible to competent authorities upon request.

9. Market contestability – Improve DMA enforcement's predictability and procedures

The Digital Markets Act (DMA) was designed as a self-executing rulebook, yet its enforcement has generated significant legal uncertainty for both designated gatekeepers and the business users and access seekers who depend on predictable DMA compliance outcomes.

The Commission's interpretation in specification proceedings has at times appeared to go beyond the letter of the law, effectively introducing substantive obligations that were not foreseen by the legislature. Indeed, it appears the Commission is reshaping the DMA's scope through enforcement rather than the legislative process. While this discretionary approach is harmful to gatekeepers' ability to plan and invest, it also disadvantages business users and access seekers: when compliance expectations shift unpredictably mid-process, the interoperability and access arrangements they rely on become equally unstable, delaying the very contestability outcomes the DMA was designed to deliver.

The regulatory dialogue, meanwhile, has lacked the transparency and structure necessary to support effective compliance on any side – focusing more on identifying potential non-compliance than on providing clear direction on what compliant solutions would look like in practice. Procedural deficiencies compound this uncertainty in ways that affect the entire ecosystem.

Unlike antitrust and merger-control proceedings, the DMA provides no automatic right to an oral hearing and no access to an independent hearing officer to resolve disputes over confidentiality or access to the case file. The six-month timeline for specification procedures is structurally insufficient: designated companies only receive preliminary findings and access to the case file at the three-month mark, leaving just 90 days to analyse complex technical and legal findings, to assess their implications for intellectual property, security, and privacy, and to prepare a substantive response.

Rushed or poorly examined compliance solutions are not in the interest of gatekeepers, nor others. They risk producing interoperability or access arrangements that are technically fragile or legally uncertain, directly harming the business users and developers who depend on them. Predictability and procedural fairness are equally vital for smaller business users using gatekeeper infrastructure, whose own compliance operations and commercial planning rely entirely on the stability of those interoperability conditions.

Furthermore, the interaction between the DMA and national competition law adds a further layer of complexity: the possibility of parallel investigations by national competition authorities on the same matters imposes multiplied burdens and risks diverging enforcement outcomes without improving outcomes or contestability for any market participant.

Call to action: The Commission should **issue guidelines clarifying compliance expectations for Articles 5, 6, and 7, taking into account the diversity of business models subject to the DMA**, and ensure that specification decisions are strictly limited to clarifying existing obligations rather than introducing new substantive requirements. The **DMA should be amended to introduce an automatic right to an oral hearing and access to an independent hearing officer**. Specification procedure timelines should be extended to allow for meaningful engagement with preliminary findings, including their implications for intellectual property, security, and privacy. Finally, the Commission should also **issue guidelines on Article 1(6) clarifying the division of responsibilities between the Commission and national competition authorities,** granting itself the explicit authority to pause national investigations when specification proceedings or compliance negotiations are underway.

III. Resolving direct legal frictions & sectoral creep

Conflicting mandates across different EU laws place businesses in legal deadlocks. Clear hierarchies are needed to restore certainty for digital services and the wider ecosystem.

10. Data protection – Resolve the GDPR and ePrivacy dual-consent deadlock

The EU currently operates a contradictory, two-tier data governance framework where the outdated ePrivacy Directive continuously clashes with the GDPR's nuanced, risk-based approach. Originally adopted in 2002 and designed for a fundamentally different technological era, the ePrivacy Directive predates the GDPR by nearly a decade.

Despite long-standing commitments to modernise it, the Directive remains in force, imposing a parallel architecture that generates profound legal uncertainty, drives up compliance costs, and severely undermines the coherence of Europe's digital rulebook.

The core of this structural duplication lies in a direct conflict over the legal bases for data processing. The GDPR establishes a comprehensive framework that calibrates compliance to the actual severity of the activity, offering a balanced set of legal bases – including 'legitimate interest' and 'contractual necessity'. By contrast, the ePrivacy Directive overrides this framework for electronic communications and terminal equipment access by imposing a rigid, near-absolute consent requirement.

Consequently, today businesses are still trapped between two overlapping regimes with no authoritative mechanism to resolve the friction. This leaves them unable to determine in good faith whether processing explicitly permitted by the GDPR under legitimate interest (Article 6(1)(f)) is simultaneously blocked by the ePrivacy Directive.

This categorical mandate strips away necessary flexibility and creates severe practical frictions that actively harm both users and businesses. Most visibly, it has fueled an

ecosystem defined by ubiquitous consent banners that causes user fatigue, undermining the very user autonomy the Directive originally aimed to protect.

Furthermore, because the Directive restricts terminal equipment access regardless of whether personal data or actual privacy risks are involved, it creates disproportionate roadblocks for critical, non-intrusive functions like security, fraud prevention, and network integrity. It also enforces a strict opt-in requirement for electronic direct marketing, creating an unjustified asymmetry between online and offline marketing that completely bypasses the GDPR's established balancing tests.

Call to action: The Commission should use the Digital Fitness Check to commit to a **clear legislative roadmap that phases out the ePrivacy Directive, replacing it with a single, GDPR-aligned Regulation to prevent further national gold-plating**. Pending this full legislative overhaul, the Commission must mandate the EDPB and national authorities to issue binding joint guidance that explicitly resolves the dual-consent deadlock. This interim guidance must formally permit the use of the GDPR's legitimate-interest framework for low-risk processing; specifically for analytics, security, fraud prevention, and direct marketing. It should explicitly remove the consent requirement for terminal equipment access where no personal data is involved or where access is strictly necessary for network integrity.

11. Content moderation – Halt sectoral creep undermining the DSA's monitoring ban

The Digital Services Act (DSA) established a clear horizontal framework that provides vital liability protections for online intermediaries, such as strictly prohibiting general monitoring obligations (Article 8). However, this foundational principle is constantly undermined by creeping sectoral legislation attempting to institute proactive vetting via the backdoor.

Recent EU proposals and rules – ranging from the Customs Union Reform and Payment Services Regulation (PSR) to the Medical Device Regulation (MDR) and the General Product Safety Regulation (GPSR) – increasingly pressure platforms to substantively vet third-party apps or proactively monitor product interfaces for sector-specific compliance.

This relentless sectoral creep creates severe legal uncertainty, effectively forcing online intermediaries and commerce infrastructure providers into the role of specialised regulators — a role they are neither legally mandated nor technically equipped to play. When sectoral rules attempt to hold platforms liable for the substantive compliance of the millions of third-party developers or merchants they host, it bypasses the DSA's carefully calibrated liability safe harbours and threatens the viability of the Digital Single Market. Furthermore, imposing these unworkable obligations risks creating massive barriers to entry for smaller merchants and businesses that rely on digital platforms to access the Single Market.

The same dynamic risks emerging where DMA enforcement targets measures that gatekeepers have put in place specifically to combat spam and deceptive content — conduct that the DSA independently requires platforms to mitigate as part of their 'systemic risk' obligations. By treating such measures as potential competition violations, the Commission risks placing gatekeepers in an impossible position: dismantling user

protections to satisfy DMA enforcement could simultaneously expose the same platform to DSA liability – a conflict the current rulebook provides no mechanism to resolve.[9]

Call to action: The Commission must **establish a formal 'governance check' during the interservice consultation phase, explicitly empowered to strike down or amend any sectoral legislation that attempts to rewrite horizontal intermediary liability principles**. Furthermore, existing and future sectoral legislation must include explicit carve-outs reaffirming that intermediaries are not subject to general monitoring or proactive vetting obligations.

12. Media – Reconcile conflicting DSA & EMFA content-moderation mandates

The recently enacted European Media Freedom Act (EMFA) introduces severe legal friction with the DSA's core risk mitigation framework, placing platforms in an impossible compliance paradox. While the Digital Services Act strictly mandates Very Large Online Platforms (VLOPs) to act swiftly to mitigate 'systemic risks' – such as the rapid spread of illegal content or coordinated disinformation – the EMFA's Article 17 introduces specific 'media privilege' obligations, which force platforms to delay moderation actions and provide advance warnings to self-declared media service providers before being allowed to restrict content.

This contradiction effectively catches companies between the DSA's mandate to act immediately and the EMFA's obligation to delay action. Beyond the administrative compliance deadlock, this friction opens dangerous loopholes for malicious actors and state-sponsored disinformation campaigns, who can easily exploit the system by masquerading as legitimate media entities to shield their content from rapid takedowns.

The EU's digital rulebook cannot demand immediate systemic risk mitigation while simultaneously legislating mandatory moderation delays. While the Commission's recent EMFA guidelines clarify the procedural aspects of media self-declarations, they fail to address this substantive clash of legal mandates.

Call to action: As the sole enforcer of the DSA for VLOPs, the Commission should **issue formal assurances that platforms prioritising the rapid mitigation of systemic risks, such as coordinated disinformation efforts, will not face regulatory penalties for overriding the EMFA's delay mandates**. Ultimately, the Digital Fitness Check must lead to a targeted legislative amendment clarifying that Article 17 of EMFA is strictly without prejudice to a platform's overarching risk mitigation obligations under the DSA.

13. E-Commerce – Ensure alignment between the DSA and other sectoral rules

Achieving a coherent regulatory landscape for online safety is crucial, yet current overlaps between the Digital Services Act (DSA) and other legislation – such as the GDPR, Audiovisual Media Services Directive (AVMSD), Unfair Commercial Practices Directive, Consumer Rights Directive, or the Artificial Intelligence Act – risk undermining this

[9] The DSA requires very large online search engines to identify and mitigate systemic risks, including the amplification of manipulated or deceptive content (DSA Article 34). In November 2025, the Commission opened a DMA investigation into Google's Site Reputation Abuse Policy (SRAP), an anti-spam measure introduced in response to escalating manipulation of search rankings. See Nextrade Group, Trust, Safety, and Competition (February 2026) https://www.nextradegroupllc.com/dma-s-security-implications

effectiveness.[10] While the existing legal framework established through the DSA already provides an adequate basis for online safety, the primary challenge lies in the inconsistent application of these rules. This ambiguity has allowed for a patchwork of diverging Member-State initiatives that depart from a unified EU framework, escalating legal and business uncertainty for service providers.

For example, when it comes to the Digital Services Act's interaction with the AVMSD, its focus on video-sharing and audiovisual content meets the DSA's broader horizontal obligations. For Very Large Online Platforms (VLOPs), this complexity is compounded by the systemic-risk assessment obligations (Articles 34 and 35 DSA), which require a holistic approach that may clash with granular, sector-specific national requirements.

Similarly, the DSA's advertising transparency provisions (Articles 26 and 39) are currently undermined by an overbroad definition of 'advertisement' in Article 3(r), which risks capturing routine commercial features such as price reductions, promotional discounts, or featured placement of a merchant's own products, which are already governed by the Price Indication Directive and the Unfair Commercial Practices Directive. Subjecting the same commercial practices to parallel DSA advertising transparency obligations – with distinct labelling, repository, and record-keeping requirements – imposes duplicative compliance costs on platforms and merchants without delivering additional consumer benefit.

The DSA's trader-traceability obligation (Article 30) raises a similar proportionality concern. Platforms enabling distance contracts must collect and display specific trader information, including telephone numbers and email addresses. Yet on many marketplaces and service platforms, traders include individual entrepreneurs and micro-businesses that do not maintain separate professional contact details. Requiring these individuals to disclose personal phone numbers and home addresses to the general public – irrespective of the trader's size, the nature of the transaction, or the availability of alternative contact mechanisms already provided by the platform – constitutes a disproportionate intrusion on their privacy that is not in line with the GDPR's data minimisation principle and could put operators of small and medium enterprises at risk, instead of empowering them.

Call to action: Rather than introducing new layers of obligations, **any new legislation that touches upon online safety should prioritise absolute alignment with the horizontal framework established by the DSA** to ensure a coherent and effective regulatory landscape. That includes, for example, the upcoming AVMSD review and Digital Fairness Act (DFA). The European Commission should focus on enforcing a unified interpretation of existing laws across all Member States to prevent the current patchwork of national initiatives from further fragmenting the Digital Single Market. Improving consistency and legal certainty in this manner is the only way to ensure that industry-wide solutions for online safety are both effective and universally applied.

The Commission should also **clarify, through implementing guidance or a targeted amendment, that the concept of 'advertisement' under Article 3(r) DSA does not extend to standard commercial features** such as price reductions, discounts, or terms of sale for

[10] As noted in the Commission's Report on application of Article 33 of the DSA and the interaction of that Regulation with other legal acts, available here: https://digital-strategy.ec.europa.eu/en/library/report-application-article-33-regulation-eu-20222065-dsa-and-interaction-regulation-other-legal

goods and services directly transacted through a platform's primary interface, which are already adequately regulated under existing consumer protection instruments. Finally, the Commission should **introduce a proportionality test within Article 30 DSA, enabling platforms to fulfil trader traceability through alternative means** – such as verified in-platform messaging – where public disclosure of personal contact details would be disproportionate.

14. Intellectual property – Prevent automatic injunctions and ensure FRAND licensing

After more than twenty years, the Directive on the Enforcement of Intellectual Property Rights (IPRED) is no longer fit for purpose, failing to support innovators in critical growth areas like artificial intelligence and semiconductors. While IPRED mandates that enforcement measures should be proportionate, the Commission's own studies confirm that this requirement is routinely ignored in patent cases, with injunctions being granted in 99% of cases without meaningful proportionality assessment.[11]

This legal imbalance makes Europe's current legal framework an increasingly attractive hunting ground for patent assertion entities (PAEs) – also known as 'patent trolls'. It forces innovative companies to pay far more than a patent is actually worth simply to avoid the catastrophic risk of having their products pulled from the market. Ultimately, this creates disincentives for investment in vital technologies such as 5G, AI, and semiconductors – shifting critical resources away from research and development towards payments to shell entities that produce nothing of their own. [12]

This distorted landscape is particularly damaging for standardised technologies like 5G or WiFi. European businesses seeking to innovate on top of these standards face a lack of transparency regarding licensing costs and must negotiate under the constant cloud of an injunction threat. Although patents essential to a standard, so-called standard essential patents (SEPs), are supposed to be available on fair, reasonable, and non-discriminatory (FRAND) terms, the current lack of an appropriate legal framework has turned the EU into a global hotspot for SEP litigation. By falling behind other jurisdictions in addressing these systemic imbalances, the EU is inadvertently creating a barrier for companies in the EU striving to innovate, grow, and create employment opportunities within the Single Market.[13]

Call to action: To allow innovators to focus on product development rather than navigating an opaque legal landscape, the Commission must **initiate a targeted reform of IPRED to end the automatic granting of injunctions in patent cases** and better enforce the principle

[11] European Commission: Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Follow-up study on the application of the Directive on the Enforcement of Intellectual Property Rights, Publications Office of the European Union, 2026, https://data.europa.eu/doi/10.2873/9680583; European Parliament, Priority question for written answer from MEP Marion Walsman to the Commission, https://www.europarl.europa.eu/doceo/document/P-10-2025-002859_EN.html, 14 July 2025.

[12] CCIA Joint letter to EVP Stéphane Séjourné on the IPRED modernisation, https://ccianet.org/library/joint-letter-to-evp-stephane-sejourne-on-the-ipred-modernisation/, 3 March 2026.

[13] CCIA Europe, Standard Essential Patents in the EU: How Outdated SEP Regulation Hurts Innovation, https://ccianet.org/articles/standard-essential-patents-in-eu-how-outdated-sep-regulation-hurts-innovation/, 29 March 2024.

of proportionality. This modernisation should be coupled with a robust framework and clearer, actionable rules for the transparent and fair licensing of SEPs.

IV. Strengthening governance & future rulemaking

The long-term success of the digital rulebook depends on unified enforcement mechanisms, regulatory cooperation, and a strict commitment to evidence-based policymaking.

15. Governance – Implement the AI Act proportionately, moratorium on new regulation

For Europe to truly become the 'AI continent' the Commission aspires it to be, implementation of the AI Act needs to be better balanced and reflect the spirit of the EU's simplification and competitiveness agendas. New premature regulations must be avoided at all cost in order to maintain legal certainty and boost AI adoption across the EU.

The current threshold for general purpose AI (GPAI) models posing a 'systemic risk' – currently set at 10^{25} floating-point operations (FLOPs) – is outdated and does not reflect today's technology. This metric was established by EU co-legislators late in trilogue negotiations without any rigorous technical or economic impact assessment, and now captures commonplace commercial models that pose no actual systemic risk. To accurately reflect the risk profile of frontier models and avoid sweeping in basic commercial tools, this threshold must be raised to reflect the state of the art.

Enforcement powers and classification mechanisms under the Act also require recalibration in order to protect European intellectual property. Article 74(13) grants market surveillance authorities unprecedented access to proprietary source code, creating severe cybersecurity vulnerabilities and threatening trade secrets across 27 Member States, when in practice standard output testing and documentation reviews would suffice. Furthermore, the broad 'high-risk' classification in Annex III inadvertently risks capturing basic, rule-based software systems that apply deterministic logic without any machine learning components. Lacking any binding implementing acts for the time being that explicitly exclude these low-risk tools, the AI Act risks hampering conventional software development.

Compounding these substantive issues is the looming threat of Single Market fragmentation and compliance fatigue. The AI Act currently lacks a robust mutual recognition framework, leaving companies highly vulnerable to duplicative, country-by-country conformity assessments. As the European Commission's AI Office and national authorities will spend the next several years building this complex supervisory architecture and finalising technical standards, the ecosystem requires absolute regulatory stability in the meantime. Introducing any further AI-specific horizontal regulation before the current framework is fully implemented and rigorously assessed would therefore trigger a massive compliance deadlock and undermine the Act's core objective of providing predictability.

Call to action: The Commission must use the Digital Fitness Check to **commit to a strict moratorium on any new AI-specific horizontal regulation until the current framework is fully operational** and its economic impacts are formally reviewed. The Commission should also adopt a delegated act raising the GPAI 'systemic risk' threshold to reflect the state of the art, issue implementing acts that establish an EU-wide mutual recognition framework

for conformity assessments, and explicitly exempt deterministic, rule-based systems from Annex III high-risk classifications. Finally, co-legislators must amend or heavily restrict Article 74(13) of the AI Act to ensure source-code access is strictly limited to a last resort measure that is subject to judicial oversight and robust trade-secret protections equivalent to competition law proceedings.

16. Single Market – Ensure 'one-stop-shop' and 'country of origin' across borders

The integrity of the European Union's Digital Single Market is continually undermined by national-level 'gold-plating' of directives that apply to the digital sector. Despite the aim of EU-wide harmonisation, the fragmented transposition and enforcement of frameworks such as NIS2 and eIDAS 2.0 create massive legal and administrative barriers.

Indeed, startups and scale-ups attempting to offer cross-border services are forced to navigate 27 distinct national compliance regimes rather than a unified EU rulebook, severely crippling European competitiveness and duplicating compliance costs.

Fragmentation is further exacerbated when the 'country-of-origin' and 'one-stop-shop' principles are weakly enforced or bypassed entirely by national authorities issuing diverging, localised interpretations of EU law. When digital companies cannot rely on the supervision of a single lead authority in the Member State of their main establishment, the foundational promise of the Single Market – to allow seamless cross-border operation and scaling – is broken.

This fragmented oversight increases the likelihood of contradictory requests and diverging interpretations of the exact same system across the EU. For digital service providers and platforms enabling cross-border sales, this lack of coordination translates directly into inconsistent user and business onboarding, data governance, compliance reporting, and consumer protection processes – thus eroding the Single Market's integrity.

Call to action: The Commission must **strictly enforce the 'country-of-origin' and 'one-stop-shop' principles across all digital frameworks**. Enforcement powers must be exclusively vested in the lead authority of the Member State where the company has its main establishment to ensure that an entity's compliance assessment is valid across the entire EU. Where Member States diverge from these principles through inconsistent transposition or unauthorised localised enforcement, the Commission should use all available tools to ensure uniform application – including guidance, coordination through relevant supervisory bodies, and, where necessary, enforcement action.

17. Cooperation – Establish baseline enforcement rules for regulatory authorities

As the EU digital rulebook expands, the boundaries between the various legal frameworks – data protection, competition, consumer protection, artificial intelligence, and cybersecurity – are increasingly blurring. Some of the most recent legislation has begun to acknowledge this reality, attempting to manage specific intersections through dedicated coordination bodies and cooperation mechanisms (e.g. the European Board for Digital Services under the DSA, the DMA's High Level Group, and the European Data Innovation Board under the Data Act).

However, such efforts unfortunately remain the exception rather than the norm, and even where they do exist, their maturity, scope, and statutory power vary considerably. The vast majority of EU digital laws continue to handle enforcement exclusively among relevant authorities within a given field, leaving cross-sectoral conflicts entirely unaddressed. What the rulebook conspicuously lacks, across the board, is any procedural authority to manage conflicts during active, cross-border enforcement cases – precisely the moment when coordination matters most.

This gap is increasingly consequential. Regulatory bodies are progressively stepping outside their traditional purviews to interpret and enforce rules that fall outside their primary mandate, without any obligation to coordinate with the authority principally responsible for those rules. The paradigmatic example is a competition authority grounding an abuse-of-dominance finding in a determination that a company has breached the GDPR – effectively making binding data-protection findings without the institutional expertise, procedural safeguards, or accountability mechanisms that data protection law requires.[14]

This dynamic is not confined to any single framework: consumer, telecom, labour, digital services, consumer, and AI authorities are equally capable of – and increasingly inclined towards – making incidental findings under rules that belong to another supervisory regime. The result is not merely procedural inefficiency. It produces contradictory legal interpretations of the same underlying conduct from different authorities, and leaves companies and markets without authoritative guidance on which interpretation prevails.

When multiple authorities claim competence over the same digital practice without a formalised coordination mechanism, legal certainty collapses. Companies face the untenable position of defending identical business conduct against diverging legal interpretations from different authorities, potentially incurring compounding penalties for a single alleged infringement; an outcome that raises serious questions of compatibility with the 'ne bis in idem' principle. This is not solely a problem for the companies concerned: incoherent enforcement outcomes erode regulatory predictability for all market participants, distort the level playing field across the Digital Single Market, and ultimately undermine the policy objectives that each individual framework was designed to achieve. The current rulebook contains no structural safety net against this governance failure whatsoever.

Call to action: The Commission should use the Digital Fitness Check to **propose horizontal, baseline rules enshrining the principle of sincere cooperation among all national and EU regulatory authorities with competence over digital markets**. At the enforcement level, the EU needs a binding coordination framework that legally **requires any investigating authority making findings under rules outside its primary mandate to notify and consult the designated lead authority at the outset of its investigation**. A clear sequencing mechanism should prevent divergent findings on the same conduct, and where a lead authority has already established an authoritative interpretation of the rules it is responsible for, secondary authorities should be required to seek a binding opinion before departing from it.

[14] See Case C-252/21, Meta Platforms Inc. and others v. Bundeskartellamt, https://curia.europa.eu/juris/document/document.jsf;jsessionid=8462F5F83062862AD627F9EAD59D25D7?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1299124

This framework should apply horizontally across all areas of the digital acquis – competition, data protection, consumer protection, AI, cybersecurity and beyond – ensuring that the proliferation of enforcement actors translates into coherent, rather than contradictory, outcomes across the Single Market.

18. Better regulation – Mandate impact assessments for late-stage legislative changes

The unworkable complexity of the current digital rulebook is largely the result of systemic flaws in the EU legislative process itself. Too often, massive and completely unassessed changes are introduced late in opaque interinstitutional trilogue negotiations, fundamentally altering the scope and operational reality of the original legal texts. Recent flagship files, such as the AI Act and the Data Act, were subjected to expansive political compromises at the eleventh hour without any accompanying technical or economic feasibility checks.

This procedural shortcut bypasses Better Regulation guidelines and results in asymmetric, contradictory rules that drain engineering resources and stifle innovation. As highlighted by recent competitiveness reports, European innovation cannot be sustained if the rulebook is built on late-stage political compromises reached without adequate technical scrutiny, rather than rigorous, evidence-based impact assessments.

When the operational reality of tech regulation is decided behind closed doors without expert or industry consultation, the resulting laws are often technically impossible to implement and create overlapping, conflicting mandates.

Call to action: The Commission and co-legislators must commit to a structural reform of the interinstitutional agreement on better law-making. In particular, **any substantial amendment, new obligation, or expansion of scope introduced during trilogue negotiations must automatically trigger a mandatory, expedited renewed impact assessment** to guarantee technical workability and proportionality before final adoption.

Conclusion

The Digital Fitness Check comes at a pivotal moment. As the Draghi and Letta reports have made clear, Europe's competitiveness gap is real and widening. And the EU's incoherent, fragmented digital rulebook is one of its structural contributors.

The recommendations set out in this response are not requests for marginal adjustments. Rather, they address genuine legal conflicts, duplicative burdens, and enforcement gaps — spanning data governance, content moderation, AI regulation, and cybersecurity. These fundamental problems impose real costs on businesses operating across the Single Market today, from technology providers to the millions of entrepreneurs, SMEs, and merchants that rely on digital services to build, scale, and export across Europe – and beyond.

The European Commission now has the opportunity to demonstrate that the EU can regulate ambitiously and govern coherently at the same time. A simpler, more consistent digital rulebook will not only reduce compliance costs, it will restore the legal certainty that businesses need to invest, scale, and innovate in the EU, consistent with the ambitions set out in the Commission's Competitiveness Compass.

CCIA Europe stands ready to support that work with concrete technical expertise and looks forward to engaging with the Commission throughout the process.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org