CCIA Europe Response to the European Commission's Public Consultation on the Upcoming Digital Omnibus Simplification Package

# Simplifying the EU digital rulebook for innovation

**October 2025**

The Computer & Communications Industry Association (CCIA Europe) looks forward to the European Commission's upcoming Digital Omnibus Simplification Package. This timely initiative acknowledges the significant administrative burdens and compliance costs the digital sector faces due to the accumulation of overlapping, fragmented, and at times contradictory EU digital rules. Simplification should make the EU rulebook coherent, efficient, and workable to safeguard innovation and competitiveness in Europe.

## I. Improving key tech rules identified by the consultation

*In recent years, the EU's inflationist legislative output has created unprecedented complexity and fragmentation across multiple legal instruments. Looking at the areas identified by the Commission consultation, simplification must make these rules coherent and predictable.*

### Recommendations:

1. AI Act: Ensure practical and predictable application
2. Cybersecurity: Eliminate duplication and drive automation
3. Data rules: Defer mandatory standards and remove structural barriers
4. GDPR and e-Privacy: Create a unified data framework
5. eIDAS: Align and recognise global standards

## II. Fixing other, equally significant EU digital laws

*Beyond the narrow scope of the Commission's consultation, complexity and fragmentation have accumulated across the broader digital acquis, creating significant operational burdens and legal uncertainty for businesses. To achieve meaningful simplification, the Commission should also tackle these cross-cutting regulatory frictions.*

### Recommendations:

6. DMA: Tackle uncertainty and procedural flaws
7. DSA: Produce essential guidance, avoid duplication and contradiction
8. P2B Regulation: Remove redundancy and reduce resource intensity
9. Modernise the Consumer Rights Directive (CRD), fix product information frictions

## III. Addressing systemic faults to future-proof new laws

*In addition to addressing flaws in existing laws, simplification also requires Europe to design future EU digital laws with much greater coherence. Learning from past mistakes, structural reforms in lawmaking are needed to protect innovation and bolster Europe's competitiveness.*

### Recommendations:

10. Avoid repeating these three legislative patterns
11. Adopt structural reforms for future legislation
12. Learn from practice for the upcoming DNA and DFA

# Introduction

The European Commission's upcoming Digital Omnibus Simplification Package is a necessary and timely recognition of the significant administrative burdens and compliance costs imposed on the digital sector by the accumulation of overlapping, fragmented, and at times contradictory EU digital legislation.

At the Computer & Communications Industry Association (CCIA Europe), we believe that simplification must transcend mere procedural adjustments. It must fundamentally restructure the EU rulebook – and the way future laws are written – to ensure it is coherent, proportionate, and workable. This is crucial to safeguarding Europe's innovation power and competitiveness, both within the Single Market and globally.

This response to the Commission's consultation highlights the specific legislative areas facing spiralling complexity, but equally stresses that simplification must extend beyond the immediate scope of the consultation to the broader digital *acquis* in order to achieve any meaningful impact.

Past and ongoing legislative processes have created systemic traps that must be avoided in future policy design. These traps include the reliance on rigid 'one-size-fits-all' obligations, the imposition of asymmetric rules, and the setting of unrealistic implementation timelines.

The lack of timely technical standards and guidance, combined with definitional conflicts across laws like the General Data Protection Regulation and the AI Act, leaves companies facing high legal uncertainty. It also risks underwhelming enforcement because regulators are flooded with low-quality, over-reported notifications.

To make the EU framework sustainable, all regulations — past, ongoing, and future proposals – must be rigorously grounded in the realities of the markets they are intended to regulate. The following sections outline urgent and actionable recommendations across three strategic fronts:

I. Improving key tech rules identified by the consultation
II. Fixing other, equally significant EU digital laws
III. Addressing systemic faults to future-proof new laws

# I. Improving key tech rules identified by the consultation

*In recent years, the EU's inflationist legislative output has created unprecedented complexity and fragmentation across multiple legal instruments. Looking at the areas identified by the Commission consultation, simplification must make these rules coherent and predictable.*

## 1. AI Act: Ensure practical and predictable application

The optimal application of the AI Act requires predictable and consistent implementation that reduces legal uncertainty and avoids unnecessary barriers to innovation.

## Problems

The application timeline of the AI Act as currently foreseen is unworkable. Crucial legal specifications, such as the Code of Practice on Transparency (Art. 50) and the necessary technical standards, will not be complete before mid-2026, yet key provisions will already apply from August 2026. This creates high legal uncertainty as companies lack the time to prepare for compliance based on the required guidance and legal specifications.

This issue is compounded by a significant degree of definitional misalignment in the regulation of automated systems. The definitions of the General Data Protection Regulation's (GDPR) 'automated individual decision-making' (Article 22), the AI Act's 'AI system' (Article 3(1)), and the Platform Work Directive's (PWD) for automated decision-making systems often overlap. Relatedly, the GDPR's Data Protection Impact Assessments (DPIAs), the AI Act's Fundamental Rights Assessments (FRAs), and the PWD's reporting requirements all cover similar issues and entail similar – but partially misaligned – obligations. This fragmented landscape results in legal uncertainty, duplicative compliance burdens, and conflicting obligations for AI providers and platforms alike.

Furthermore, many positive AI use cases, such as those that enable helpful customer interactions or the analysis of images, pose no significant risk of harm, yet risk potential over-classification under Article 6(3). For instance, certain risk categories – such as emotion recognition – could capture beneficial and low-risk applications, like a customer chatbot adapting to or routing frustrated customers.

As for enforcement, the reliance on national market surveillance authorities (MSAs), without an obligation for them to align their activities, creates a significant risk of fragmented interpretations and enforcement across the EU. In addition, the reliance on various authorities – including data protection authorities (DPAs), national labour inspectorates, and MSAs – for the AI Act creates fragmented oversight, which increases the likelihood of contradictory requests and diverging interpretations of the same system.

And although the AI Act is supposed to be without prejudice to EU copyright law as set out in the Copyright Directive, certain of the AI Act's provisions directly conflict with applicable EU copyright *acquis* and international law. For example, a mere Recital (106) in the AI Act seems to extend EU copyright law to all other jurisdictions, which runs against the fundamental territoriality principle of copyright.

## Solutions

To solve these issues, the first priority should be to **delay AI Act implementation until at least 12 months after relevant guidance, codes of practice, or technical standards become available**. This should be coupled with **aligning CEN/CENELEC's technical standards with international frameworks** (e.g. OECD, G7).

The Commission should also **ensure a coherent definition of automated systems across the digital rulebook**, or at the very least provide clarifying guidelines to authorities on how to interpret and deal with definitional gaps and overlaps.

To reduce unnecessary burdens, the exceptions in Article 6(3) should **exempt systems that do not pose a significant risk of harm**, such as emotion recognition for market research, and Article 49(2) should be available for systems that pose no significant risk of harm, even if they do not fall directly within enumerated high-risk conditions.

Additionally, to resolve the overlap in reporting – where the GDPR's DPIAs, AI Act's FRAs, and PWD's reporting requirements all cover similar issues – AI providers should be able to determine whether a DPIA suffices for FRA requirements to reduce duplicate work.

To avoid conflicts with copyright laws outside the EU, the Omnibus should remove relevant parts of Recital (106) of the AI Act extending EU copyright rules outside its jurisdiction.

Finally, to combat fragmented enforcement, the Commission should establish a transparent mechanism for mutual recognition of MSAs' decisions for high-risk AI systems. There is also an urgent need to define a Union-wide collaboration framework among relevant enforcement authorities i.e. DPAs, national AI regulators, and national labour authorities to create a harmonised oversight of the implementation of regulations related to 'automated decision making' and prevent conflicting interpretations.[1]

## 2. Cybersecurity: Eliminate duplication and drive automation

Cybersecurity simplification must move beyond minor procedural adjustments. Instead it should focus on eliminating regulatory duplication and maximising opportunities for automation to ensure resources are dedicated to resilience, not administrative overhead.

### Problems

The current environment is burdened by duplicative and conflicting cybersecurity incident reporting requirements from at least seven different legislations, including the NIS2 Directive and the Cyber Resilience Act (CRA). This means that for a single incident, a business may be forced to fill out several different forms, with inconsistent requirements on data points. This duplication is an example of regulatory inefficiency, as the same technical information is reported repeatedly without improving security outcomes.

Furthermore, the lack of a uniform definition of what constitutes a reportable, major, or severe 'incident' – with different thresholds applying under NIS2, GDPR, and the Digital Operational Resilience Act (DORA) – leaves companies uncertain about when to notify. This legal uncertainty encourages over-reporting to stay on the safe side, which floods regulators with minor notifications, making it harder to focus on serious threats.

Aside from incident reporting, companies must comply with a wide range of ongoing approval and certification obligations under NIS2, DORA, CRA, and national laws. Although the objectives are similar, each Member State interprets and enforces these rules differently, leading to divergent supervisory practices. This forces companies to run duplicative audits and parallel compliance programmes, raising costs without improving security outcomes.

### Solutions

To simplify incident reporting, the **Commission must enforce a 'report once, comply many' approach**. This requires unifying templates, reporting deadlines, and severity

[1] For more details, see *CCIA Europe Response on the EU Commission Consultation on the Apply AI Strategy*, June 2025, available at https://ccianet.org/library/ccia-europe-response-eu-commission-consultation-on-the-apply-ai-strategy/;

thresholds across all relevant legislative acts (NIS2, CRA, DORA, GDPR, etc.) to establish a common and aligned understanding of regulatory requirements.

The ultimate goal is to **create a single EU-level reporting platform with automation**. This platform should be designed for interoperability, so companies can integrate reporting directly into their security operations systems. Finally, standardising classification guidelines and key definitions – e.g. clear, quantifiable thresholds based on duration, number of users affected, or economic loss – would reduce administrative burden and provide regulators with higher-quality, comparable data.

Beyond incident reporting, and to help compliance with security measures, the European Commission should propose: (1) harmonising obligations to establish one robust security framework across the EU; (2) providing clear EU-level guidance to ensure consistent supervision which would reduce interpretative gaps during audits; and (3) standardising compliance reporting formats to allow companies to prepare one comprehensive audit package that satisfies multiple authorities.

All of this needs to be complemented with a clear commitment to **enforce the intent behind the NIS2 'one-stop-shop' mechanism** to ensure that entities are registered and supervised by only a single Member State. The one-stop-shop mechanism should be extended to all relevant applicable laws (e.g. the European Electronic Communications Code (EECC)) and combined with mutual recognition provisions. This would help ensure that an entity's compliance assessment by its responsible authority is valid for other EU Member States' authorities, including comparable sectoral regimes, thereby reducing cross-border friction.

To strengthen Europe's cyber resilience, certification and security measures must be consistent, practical, and interoperable. Currently, Member States are developing their own certification schemes and supply chain assessments, creating an unmanageable tangle of obligations that are often duplicative or contradictory. This fragmentation makes it harder for authorities to consistently assess systemic risks.

The upcoming Omnibus should also consolidate national certification schemes into single, clear EU-level technical frameworks. Furthermore, the EU should **invest significant efforts in engaging in mutual recognition agreements with third countries, and align with international approaches** such as NIST CSF and ISO/IEC 27001. Requiring companies to duplicate evidence for EU purposes wastes resources and makes the EU a less attractive market for international operators. This is particularly critical as new standards for the CRA are being developed, and recognising existing international frameworks is essential to prevent new hardware and software products being stalled by backlogs of conformity assessment body reviews.

Relatedly, the Commission should limit the use of common specifications (CS) to truly exceptional cases, where European standard organisations decline standardisation requests. CS severely lacks the necessary guardrails and governance processes and its generalisation in the proposed Omnibus IV should be reversed entirely. The absence of oversight and consensus-based approval risks market fragmentation, reduced stakeholder participation, and the creation of regulatory barriers between the EU and international markets.

Finally, the promotion of automated evidence mapping, leveraging machine-readable formats, will allow companies to re-use security evidence across multiple frameworks and share it digitally.

## 3. Data rules: Defer mandatory standards and remove structural barriers

Simplification of the EU's data-related rules (e.g. the Data Act, Data Governance Act, Free Flow of Non-Personal Data Regulation, Open Data Directive) must focus on reducing the fragmentation and complexity that disproportionately affects innovative companies trying to scale data-driven business models. Today's implementation approach for the data *acquis* risks creating significant new barriers and legal contradictions.

### Problems

First, the European Commission plans to mandate compliance with specified interoperability standards for certain data processing services under EU Data Act Article 35, despite an absence of evidence of market failure and limited stakeholder consultation.

The Data Act's gatekeeper restrictions also create an impossible legal conflict. Article 5(2) of the Act prohibits gatekeeper-designated companies under the Digital Markets Act (DMA) from receiving user data, including personal data. This directly conflicts with the user's right to data portability under GDPR Article 20 and the portability obligations under DMA Article 6(9).

A company receiving a portability request may interpret the Data Act as requiring it to decline the transfer to a gatekeeper, thereby risking non-compliance with the GDPR or DMA. This effectively deprives individuals of controlling their personal data and results in user lock-in, limited competition, and reduced contestability.[2]

Regarding government access to company data (B2G sharing), the Data Act introduces obligations for companies to provide data to public sector bodies under certain circumstances. However, the definition of 'exceptional need' remains highly subjective, potentially creating an endless cycle of reporting and data sharing, thereby imposing undue burdens on companies.

Furthermore, rules on international governmental access and transfers (Article 32) remain too imprecise, giving significant leeway for national enforcement authorities to apply different standards for personal and non-personal data transfers outside the European Union, potentially erecting new data flow restrictions.

Separately, the Data Governance Act (DGA) imposes a rigid structural solution: it requires data intermediation services to establish a separate legal entity (Article 12) to ensure neutrality. This mandatory structural separation creates significant operational and financial burdens for companies and has a deterrent effect on data intermediation service providers. It would require substantial legal and administrative costs to establish and maintain separate entities, fragmenting existing efficient service delivery models.

[2] See *CCIA Europe letter to EU Commission on Data Act and DMA*, June 2023, available at https://ccianet.org/library/ccia-europe-letter-to-eu-commission-on-data-act-and-dma/; and *CCIA Europe letter to EDPB on Data Act and GDPR*, June 2023, available at https://ccianet.org/library/ccia-europe-letter-to-edpb-on-data-act-and-gdpr/;

This requirement creates artificial barriers between complementary services that currently benefit from integrated operations, forcing companies to duplicate infrastructure, personnel, and compliance mechanisms.

### Solutions

With respect to the Data Act, the European Commission should **first defer mandatory standards adoption under Article 35 to starting with a voluntary and informative list of interoperability standards** (similar to the approach of the Interoperable Europe Act), until clear market necessity is established following a thorough impact assessment.

To resolve the gatekeeper conflict, the **Data Act must be modified to remove gatekeepers' ineligibility to receive user data** under Article 5(2). Alternatively, the Commission and European Data Protection Board (EDPB) must issue guidelines clarifying that GDPR Article 20 takes precedence and that companies cannot be held liable under the Data Act for fulfilling a user's portability request to a gatekeeper.

Regarding government access to data (B2G), the **definitions of 'public emergency' and 'exceptional need' must be clarified** to avoid imposing undue burdens on companies.

For data flows (Article 32), the Commission should consider **introducing a presumption of lawful transfers aligned with GDPR data transfer rules** to provide legal certainty. Indeed, compliance with GDPR provisions to transfer personal data should be recognised as a means to comply with Article 32(1) of the Data Act.

For the DGA, the Commission should replace the mandatory structural separation requirement with less burdensome organisational measures and internal controls to ensure service neutrality. These measures should include mandating transparent pricing mechanisms and creating technical and operational safeguards to prevent conflicts of interest, allowing organisations to focus on delivering effective services rather than complex corporate restructuring.

## 4. GDPR and e-Privacy: Create a unified data protection framework

To reduce the legal uncertainty and unnecessary administrative burden related to data and privacy rules, the European Commission must pursue targeted reforms that ensure the consistent application of the GDPR across the full spectrum of EU digital legislation, thereby creating a unified and consistent legal regime.

### Problems

The current landscape for data protection is increasingly undermined by fragmented implementation, diverging national interpretations, and overly rigid guidance at EU level. This complexity is further exacerbated by definitional conflicts with new legislation.

For example, and as mentioned earlier in the AI Act recommendations, the concept of 'automated decision-making' is defined in different ways in Article 22 of the GDPR, Article 86 of the AI Act, and Articles 9-11 of the Platform Work Directive, thus creating overlapping requirements and raising legal uncertainty.

This reality directly impedes the EU's ambitions for AI leadership. The current application of the GDPR, for example, creates significant administrative burdens that slow down AI

development. Large language models are trained on vast amounts of public information, a process similar to how search engines operate.

However, conflicting approaches from national data protection authorities on fundamental issues (like the lawful basis for web scraping and the use of legitimate interest for AI training) create significant risks, delay product launches, and threaten to become a strong impediment to the adoption of advanced AI in Europe.

Other misalignments between GDPR and the Data Act persist. As mentioned above, the Data Act has introduced tangible and potential tensions with the GDPR, including when users seek to move their data to a service operated by a DMA-designated gatekeeper (e.g. virtual assistant), allowing overly broad government data access requests at home, while giving significant leeway for national authorities to apply different standards for personal and non-personal data transfers outside the European Union.

Separately, the current rules on cookies under the e-Privacy Directive require separate consent for a wide range of tracking technologies, creating legal uncertainty and fragmentation as implementation varies across the 27 EU Member States. This is particularly disruptive, as recent EDPB guidance has exacerbated the problem by broadening the application of Article 5(3) of the ePrivacy Directive – requiring GDPR-standard consent without consistent exemption guidance, leading to widespread consent fatigue.

This regulatory friction imposes a disproportionate compliance burden and severely undermines personalised advertising, a key driver of innovation and competitive pricing. This is particularly true for SMEs and smaller companies that CCIA Europe's Members serve and partner with. The frequent and disruptive pop-ups generated by these mandates cause potential customers to abandon websites, which directly impacts sales.

Internal data demonstrates the profound effect of these burdens on digital competitiveness across the ecosystem, showing that the interruption caused by cookie banners can lead to nearly 50% (45.67%) fewer high-quality sessions and a 46.45% lower conversion rate for smaller digital operators compared to larger platforms.

Finally, while prior recent effort to simplify the GDPR is welcome, pursuing lower compliance standards solely for mid-caps risks creating weak links in the supply chain, heightening the risk of supply chain attacks, and potentially leading to double standards of data protection for the same data processing activities depending on the size of the company carrying them out.

## Solutions

The first step to tackle these overlaps must be **mandating genuine, structured cooperation between the various EU and national regulators** through the establishment of a forum that brings together digital regulators for a structured sharing of information. Authorities should collaboratively develop shared guidelines – subject to mandatory public consultation – on key areas of overlap. Think, for example, of definitional conflicts around 'automated decision-making', as joint guidance is instrumental to fostering a consistent understanding and application of digital regulations.

To unlock the EU's AI potential, targeted simplification of data protection rules is also essential. First, it is crucial to **reaffirm the role of legitimate interest as a lawful basis under the GDPR for responsible AI innovation**, moving beyond the non-binding EDPB opinion to provide harmonised legal certainty for AI training.

Second, the rules for processing special categories of personal data must be clarified to permit the use of manifestly public data and to explicitly recognise GPAI model development as a qualifying scientific research purpose. The AI Act's allowance for using sensitive data for bias mitigation should also be expanded to all AI systems, not just high-risk ones. Finally, to prevent administrative duplication, the EU should clarify that a single, comprehensive risk assessment, such as a GDPR DPIA, can satisfy the documentation requirements of both the GDPR and the AI Act.

When it comes to the ePrivacy 'cookie rule', the **most impactful simplification action would be to repeal Art.5(3) entirely**. The full set of GDPR legal bases would, *de facto* and *de jure*, apply to all cookie-related data processing. It would establish a single, coherent and harmonised framework. For businesses, this truly risk-based framework for cookies would focus compliance to activities with a higher-risk profile.

For users it means reserving consent to where it matters most – for instance in situations that involve online profiling. However, efforts to reduce cookie fatigue should not involve shifting to centralised and browser-level consent mechanisms. No actor should be left responsible for consent signals for the entire web ecosystem and website owners must retain the ability to engage directly with their customers.

To address e-Privacy, cookie rules should be simplified by **moving low-risk processing – such as for software updates, security, anti-fraud, and aggregated analytics purposes – into the GDPR's risk-based framework**. This alignment would establish a single harmonised framework and reduce over-reliance on consent. However, efforts to reduce cookie fatigue should not involve shifting to centralised user controls as website owners must retain the ability to engage directly with their customers.

**For international data flows, the EU must adopt further adequacy decisions and add more flexibility and consistency** regarding the mechanisms for data transfers to increase legal certainty and facilitate transfers. The Commission should also consider introducing a presumption of lawful transfers of non-personal data that are aligned with GDPR data transfer rules to provide additional legal certainty. Furthermore, the Commission needs to work with global actors to develop stronger interoperability for data flows between the EU and third countries.

Regarding GDPR simplification, the Commission must ensure that under the principle of accountability, any simplification for SMEs maintains high standards. Large company controllers, including mid-caps, must still be able to demonstrate that all processing activities — including those carried out by processors — comply with data protection rules. Following the Omnibus IV package, CCIA Europe strongly advises against the adoption of further asymmetric data protection rules or the creation of a two-tiered system of fundamental rights.[3]

[3] For more details, see CCIA Europe's input for GDPR implementation dialogue, July 2025, available at https://ccianet.org/library/ccia-europes-input-for-gdpr-implementation-dialogue/; CCIA Europe's

## 5. eIDAS: Align and recognise global standards

The implementation of eIDAS 2.0 must reduce overlapping compliance requirements and embrace international standards. It should also embrace mutual recognition in order to avoid creating a new barrier to cross-border digital service delivery.

### Problems

The new eIDAS framework creates overlapping obligations with multiple existing frameworks (NIS2, DORA, DSA, GDPR), each with distinct incident reporting requirements, compliance obligations, and enforcement mechanisms. This forces organisations to maintain separate compliance programmes and report the same incidents multiple times, increasing administrative complexity during critical incident response periods.

eIDAS 2.0 also establishes EU-specific technical standards that diverge from established international standards (ISO/IEC 27001, FIDO Alliance). This regulatory isolation requires solutions to be redesigned specifically for the EU market, limiting access to innovative global solutions and resulting in duplicate certification costs.

Furthermore, the way in which electronic identification is performed varies across Europe, and guidance for Member States to ensure uniform implementation of the eIDAS 2.0 framework is still lacking.

### Solutions

To streamline compliance, the European Commission must **establish a unified reporting mechanism allowing entities to fulfill multiple regulatory obligations through a single submission** and extend the 'one-stop-shop' principle from NIS2 to eIDAS 2.0.

To ensure global relevance, the Commission should also **prioritise alignment with international standards** (ISO, FIDO, W3C) in developing technical specifications and establish mutual recognition agreements with international certification bodies.

Finally, the Commission must **provide clear technical guidance based on international standards well before compliance deadlines** and implement a 'stop-the-clock' mechanism for eIDAS – delaying implementation until one year after standards and implementing acts are available. This will also serve to prevent fragmentation and ensure interoperability of the eIDAS framework across the Single Market, be it as a means to verify users' age for access to online services or to interact with e-government services.[4]

response to call for evidence on the General Data Protection Regulation report, February 2024, available here: https://ccianet.org/library/ccia-europe-feedback-report-on-the-gdpr/;

[4] CCIA Europe Recommendations on 'Helping Europe achieve safe and secure age-assurance solutions', February 2025, available at: :
https://ccianet.org/library/ccia-europes-recommendations-on-age-assurance/

# II. Fixing other, equally significant EU digital laws

*Beyond the narrow scope of the Commission's consultation, complexity and fragmentation have accumulated across the broader digital acquis, creating significant operational burdens and legal uncertainty for businesses. To achieve meaningful simplification, the Commission should also tackle these cross-cutting regulatory frictions.*

## 6. DMA: Tackle uncertainty and procedural flaws

The Digital Markets Act (DMA) generates significant legal uncertainty and operational burdens due to fundamental design flaws, problematic enforcement procedures, and regulatory overlap. The complexity of the DMA's provisions, coupled with the European Commission's interpretation, risks undermining legal predictability.

### Problems

First, the DMA relies on a 'one-size-fits-all' approach that fails to accommodate diverse business models. A concrete example is the data portability obligation (Article 6(9)), which, despite being designed for messaging platforms, is extended to the retail industry where customers typically do not want to move 'personal data' like purchase history.

This necessitates significant technical adaptations and financial investments. These restrictions impose substantial costs on EU businesses beyond those companies in scope of the DMA. For example, service sectors across the EU face potential revenue losses of up to €114 billion.[5] Furthermore, obligations on data portability and interoperability can create security and privacy risks if necessary safeguards are overlooked.

Second, while DMA obligations, especially under Article 5, were intended to be 'self-executing' they frequently pose implementation challenges, resulting in uncertainty. This uncertainty is compounded by the Commission's broad interpretation in specification proceedings, which has appeared to go beyond the letter of the law. This approach risks reshaping the scope and content of the DMA through enforcement rather than through the legislative process, thus undermining predictability.

Procedurally, 'gatekeeper'-designated companies have limited rights of defence during enforcement proceedings. Unlike in antitrust cases, there is no provision for an automatic right to an oral hearing or recourse to an independent hearing officer. Additionally, the six-month timeline for specification procedures is unrealistically tight, especially since gatekeepers may only gain access to preliminary findings and the case file three months into the process. Finally, the interaction between the DMA and national competition law risks regulatory fragmentation and parallel investigations by national competition authorities (NCAs) concerning Articles 1(5) and 1(6).[6]

---

[5] *Economic Impact of the Digital Markets Act on European Businesses and the European Economy*, by Cennamo, Kretschmer, Constantiou and Garcés, June 2025, available at: https://www.dmcforum.net/publications/economic-impact-of-the-digital-markets-act-on-european-businesses-and-the-european-economy/;

[6] *The Digital Markets Act: A procedural journey towards effective compliance*, King & Spalding, September 2025, available at https://www.kslaw.com/attachments/000/013/012/original/A_Procedural_Journey_Towards_Effective_Compliance.pdf?1758143009;

The DMA also creates conflicts with other EU laws, such as Article 5(2) (on data combination/cross-use) overlapping with the GDPR's consent framework, and DMA portability requirements duplicating provisions in the Data Act.

### Solutions

To enhance the DMA's predictability and workability, the **Commission should issue guidelines to clarify compliance expectations for Articles 5, 6, and 7**, considering the diversity of business models. The goal should be ensuring that the law is interpreted according to proportionality, and that specification decisions are strictly used to clarify existing obligations, not to introduce new substantive rules.

The Commission should also seek to improve procedural fairness. Specifically, the DMA should feature a **right to request an oral hearing and recourse to an independent hearing officer** to resolve disputes relating to confidentiality and access to files. Likewise, the Commission should extend timelines for specification procedures to ensure thorough consideration of the technical implications of potential measures and adequately account for the impact on intellectual property rights, security, and privacy concerns.

Last but not least, the Commission should evaluate the potential impact (on EU businesses, consumers, innovation, and IP protection) in all upcoming DMA decisions, and publish related impact assessments. It should also **clarify conflicting obligations between the DMA and other EU laws (GDPR, Data Act) and issue guidelines on Article 1(6) to clarify the division of responsibilities** between the Commission and NCAs. These guidelines should grant the Commission authority to pause national investigations when compliance negotiations or specification proceedings are underway.[7]

## 7. DSA: Produce essential guidance, avoid duplication and contradiction

To date, the Digital Services Act's (DSA) framework remains incomplete – despite the DSA becoming fully applicable to all online platforms in February 2024.

### Problems

Many crucial pieces of the puzzle are still missing, including guidelines on trusted flaggers and dark patterns, as well as a concrete methodology to count users in a uniform manner. This ambiguity is leading to inconsistencies in implementation and increased uncertainty for businesses.

Online platforms are making best efforts to comply with the principles of the law, without always having a clear direction of whether this will be perceived as enough for enforcement authorities. In addition, the DSA's transparency reports and database requirements overlap significantly, as they often use the same underlying data, creating an unnecessary operational burden.

Sectoral laws and proposals also overlap and create regulatory frictions with the DSA. For example, the provisions related to the protection of minors protection, influencer marketing, and protection of harm in the Audiovisual Media Services Directive (AVMSD) overlap with the horizontal rules established through the DSA.

[7] For more details on the DMA review, see *CCIA Europe position paper on DMA review*, September 2025, available at https://ccianet.org/library/ccia-position-paper-on-dma-review/

Furthermore, national-level initiatives 'gold-plating' EU rules introduce significant barriers across the Single Market and result in diverging levels of protection in different Member States, creating enforcement burdens and legal uncertainty for businesses operating across the Single Market.

Similarly, legislative changes extending platforms' and telcos' liability to all kinds of fraud in the Payment Services Regulation (PSR) proposal directly conflict with established principles in the DSA and are limited by the GDPR/ePrivacy Directive on information sharing. The Council's focus on fraud prevention over strict liability is a more pragmatic approach.

The European Media Freedom Act (EMFA), for its part, requires very large online platforms (VLOPs) to treat self-declared 'media service providers' (MSPs) differently in content moderation. Concretely, whoever considers itself to be an MSP is allowed to challenge moderation decisions within 24 hours.[8] The lack of clear guidelines that define a media service provider and the process for VLOPs to verify self-declarations creates a system vulnerable to abuse under the EMFA.

The overlap between the EMFA and the DSA introduces significant legal ambiguity and complexity for VLOPs, making it hard for them to determine the correct legal framework for content-moderation decisions and increasing the likelihood of contradictory interpretations between the two laws.

Finally, trilogue discussions on the proposal to reform the Union Customs Code have put forward ideas that fundamentally contradict the spirit and letter of the DSA, instituting a general monitoring obligation whereby marketplaces risk taking full liability for every imported product — from customs duties to product safety and ecodesign.

## Solutions

The European Commission must focus on a dedicated plan to **finalise all missing guidelines and technical methodologies to ensure the DSA is fully operational and harmonised**. All implementing decisions, guidelines, and technical methodologies should be adopted according to a clear calendar to ensure timely clarity. If necessary implementation steps are not finalised before the obligations they specify enter into force, the Commission should always **assess compliance as 'best efforts' and actively allocate resources to strengthen collaboration and dialogue with online platforms** struggling to navigate the persistent regulatory uncertainty.

To eliminate duplication, the regulatory framework should enable a model where platforms' data input into the centralised transparency database is used to automatically generate the mandated transparency reports.

The Commission should also **establish a clear DSA-first hierarchy to clarify mandates and achieve a coherent legal landscape** across all legislation and proposals going forward (e.g. AVMSD review, Customs Union reform, Payment Services Regulation)

Further, the upcoming Commission's evaluation of the AVSMD should aim to preserve certain key principles such as the 'country-of-origin' principle and strongly prioritise

[8] This 24-hour timeframe can be shortened in case of a public security or public health crisis (DSA Article 36)

harmonisation over a fragmented approach to national implementation and enforcement of rules.[9]

## 8. P2B Regulation: Remove redundancy and reduce resource intensity

The P2B Regulation requires platforms to have an internal system for handling business user complaints and to report on this system's effectiveness (Article 11(3)).

### Problems

However, these reporting requirements are resource-intensive and it has been proven difficult to ensure accuracy, raising questions about the value of the collected data. This is particularly redundant as the DSA now imposes equivalent obligations.

### Solutions

The Commission should **ensure that focus shifts from mandating resource-intensive reporting for every administrative data point toward a standardised, high-level set of key performance indicators** that truly measure the effectiveness of the complaint-handling mechanism. More fundamentally, the regulatory framework should merge the complaint-handling mechanism and annual reporting requirements under the DSA and P2B, or shift the P2B requirement to a reactive one for designated authorities.

## 9. Modernise the Consumer Rights Directive (CRD), fix product information frictions

The Consumer Rights Directive (CRD) requires online platforms to provide a phone number and email address as pre-contractual information (Article 6(1)(c)).

### Problems

This requirement does not reflect the reality of modern online services, which use more effective and efficient channels, such as in-app messaging systems or chatbots.

Moreover, through various pieces of legislation – such as the Packaging and Packaging Waste Regulation (PPWR), Batteries Regulation, and the Waste Electrical and Electronic Equipment (WEEE) Directive – the EU mandates extensive consumer information, resulting in fragmented and contradictory physical labelling across Member States, hindering the internal market.

### Solutions

Online services should be permitted to **implement a functional equivalence standard, allowing them to choose the communication channels that work best** for their business while maintaining accessibility and reliability. For physical goods, the **EU should prioritise digital labelling** (e.g. QR codes) to enable localised, actionable information for consumers, reduce paper waste, and enhance accessibility.

[9] More detailed CCIA Europe recommendations for the upcoming Commission's evaluation can be found here.

# III. Addressing systemic faults to future-proof new laws

*In addition to addressing flaws in existing laws, simplification also requires Europe to design future EU digital laws with much greater coherence. Learning from past mistakes, structural reforms in lawmaking are needed to protect innovation and bolster Europe's competitiveness.*

## 10. Avoid repeating these three legislative patterns

Future EU legislation must actively move away from systemic faults that have been leading to legal uncertainty, fragmentation, and disproportionate burdens on the market in recent years. Going forward, the European Commission and co-legislators should therefore avoid repeating the following patterns.

One critical pattern to avoid is **applying 'one-size-fits-all' rules and creating regulatory asymmetry**. This occurs when general rules are applied across heterogeneous business models or when regulation targets specific market players, thereby creating a 'glass ceiling' that discourages growth.

For instance, the Digital Markets Act (DMA) suffers from this fault by extending the data portability obligation (Article 6(9)) – designed primarily for messaging platforms – to the retail industry, where customers generally do not wish to move data like their purchase history. Yet designated companies must adopt broad technical and financial adaptations.

A similar asymmetric approach is evident in the proposed Space Act (EUSA), which arbitrarily segments satellite constellations based on size (e.g. 1,000 satellites), potentially discriminating against larger, non-EU operators without objective justification. More often than not, asymmetric legislation will not solve the problem(s) lawmakers purport to address, but move the problem(s) elsewhere.

A second damaging pattern is **rushing timelines without essential guidance, standards, and enforcement authority readiness**. It is both unrealistic and dangerous to assume implementation is an easy final step of the legislative process. Implementation takes time and practice to get right. The timelines agreed for implementation must account for the actual time businesses need to redesign products and processes. A clear example is the AI Act, where key provisions apply from August 2026, but essential legal specifications and technical standards will not be complete until mid-2026, creating high legal uncertainty.

Similarly, the Batteries Regulation mandates that portable batteries must be readily removable by February 2027, but final decisions on derogations are not expected until early 2026, leaving companies with an unworkable timeline of less than a year to overhaul complex product designs. Furthermore, most major pieces of tech legislation still require crucial follow-up steps, such as delegated acts or the deployment of IT tools (e.g. databases and APIs), without which regulated entities face more legal uncertainty and fragmentation.

The third pattern to avoid is **unnecessary regulation lacking evidence and transparent legislative processes**. Any proposal for new EU tech regulation should adhere to a genuine evidence-based approach, substantiated and quantified by independent sources. It is

equally important that this evidence justifies when regulatory intervention is clearly not needed.

This fault is compounded by the lack of transparency during key legislative stages, where substantial, even fundamental, changes – like new compromises – emerge late in trilogues without prior public discussion. Furthermore, elements such as compromise amendments by Members of the European Parliament are never made public, and the Council does not publish documents, diminishing the quality of the final legislation.

## 11. Adopt structural reforms for future legislation

To ensure new digital laws are simple, workable, and fair, all EU institutions must proactively adopt the following structural reforms with a view to promoting clarity and consistency.

First, the European Commission, as well as the European Parliament and the EU Council are urged to **commit to genuine evidence-based policy making and comprehensive impact assessments**. Regulation must be grounded in solid evidence, with sufficient data collected to substantiate any conclusions or proposals for intervention. If new rules are proposed, they should be deferred until clear market necessity is established following a thorough impact assessment.

Critically, any **substantial changes to a proposal, even if introduced late in trilogues, must be accompanied by an additional impact assessment** and subjected to a proportionality test to ensure workability in practice. These assessments must also consider the downstream and indirect effects on other sectors and the impact on new entrants and scale-ups.

Prioritising regulatory coherence and eliminating duplication means that lawmakers should always **carefully consider how future rules will impact the existing structure to avoid the creation of a patchwork** of overlapping and conflicting rules. If overlap is identified, new proposals should be postponed until existing rules have been properly implemented and enforced to ensure clarity and regulatory efficiency.

But this structural solution also requires enforcing a 'report once, comply many' approach across frameworks (e.g. on cybersecurity with NIS2, CRA, DORA, EECC, and GDPR), and unifying templates and severity thresholds for incident reporting. Furthermore, general rules should apply consistently across entire sectors, rather than targeting individual companies, or creating carve-outs that reduce administrative burdens for only a small segment of the economy.

**Ensure transparency, consistency, and alignment with global standards.** The EU must ensure legislative and technical processes are predictable and globally interoperable. This means that transparent legislative processes must be guaranteed, meaning all key documents should be made publicly available at every stage of negotiations.

Consistency throughout the legislative cycle is paramount, ensuring that amendments are subject to a proportionality test and that rules are designed to align with long-term objectives. Furthermore, technical standards should prioritise alignment with international

standards (e.g. ISO/IEC 27001, FIDO Alliance) to avoid requiring solutions to be redesigned specifically for the EU market.

Finally, structural solutions must include implementing a 'stop-the-clock' mechanism to delay implementation until sufficient time has passed after all necessary standards and implementing acts have been put in place, and final decisions (like derogations under the Batteries Regulation) are available.

### 12. Learn from practice for the upcoming DNA and DFA

The forthcoming Digital Network Act (DNA) and proposed Digital Fairness Act (DFA) clearly demonstrate why, going forward, the abovementioned patterns need to be avoided and structural reforms are needed for future legislation.

Indeed, the DNA proposals concerning internet traffic exchange perfectly illustrate the Commission's **failure to mandate evidence-based policy making and the risk of regulatory asymmetry.** The idea of imposing an obligation on certain popular content and application providers (CAPs) to negotiate a fee for traffic exchange with internet service providers is asymmetric and runs contrary to the net neutrality principle (Regulation 2015/2120, Article 3(3)).

Moreover, this intervention is still being considered despite numerous analyses indicating the IP interconnection market is highly functioning, driven by competitive market dynamics. The structural solution here is to avoid regulating where the market already delivers the best quality of service. Instead the Commission should support existing industry-led initiatives on data handling practices, rather than mandating specific technologies.

Likewise, the proposed DFA demonstrates the **fault of unnecessary regulation and the need for regulatory coherence.** The Act intends to tackle issues like deceptive interface design ('dark patterns'). However, this is largely redundant because existing legislation – including the DSA (Article 25), the AI Act (Article 5(1)), and the Unfair Commercial Practices Directive (UCPD) (Article 6(1)) – already contains relevant provisions to tackle these same practices.

**Instead of creating new rules, the Commission should focus on the proper enforcement of existing rules**, notably by empowering the Consumer Protection Cooperation (CPC) Network, which would yield faster and better results.

## Conclusion

The complexity confronting the European digital economy today is extremely vast – stemming from legislative fragmentation that spans core foundational EU frameworks, existing operational laws, and emerging proposals. Tackling this challenge requires a commitment to systemic change, moving beyond fragmented implementation and towards regulation that is truly coherent, proportionate, and workable.

The recommendations presented here aim not merely to lighten administrative burdens but to instill fundamental principles into EU law: mandating a 'report once, comply many' approach to eliminate duplicative requirements across cybersecurity and data laws, establishing genuine cooperation between various EU and national regulators to align

guidance on core concepts such as 'automated decision-making,' and ensuring necessary procedural safeguards are introduced to laws like the DMA.

By prioritising the stability and consistency of the EU's digital rulebook, resolving fundamental conflicts like the Data Act's potential tension with GDPR Article 20 and enforcing the use of the 'one-stop-shop' principle across frameworks, the European Commission can restore legal certainty.

Ultimately, simplification is the strategic lever that will determine the EU's ability to drive innovation and safeguard its global competitiveness. Through decisive action to fix past mistakes, stabilise the present, and future-proof its legislative processes going forward, the EU can fulfill its aspirational goal of making the digital rulebook fit for the future.

## 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