Ecommerce Europe feedback to the Call for Evidence on the Digital Fitness Check

Ecommerce Europe, the united voice of digital commerce in Europe, welcomes the opportunity to provide feedback to the Call for Evidence on the Digital Fitness Check, the second stage of the Commission's plan to simplify the EU's digital rules following the adjustments under the Digital Omnibus. We also look forward to contributing actively to other consultation activities including 'reality checks' and implementation dialogues that will take place later this year. In this feedback, we would like to underline Ecommerce Europe's key priorities for simplification of the digital acquis on specific areas particularly relevant to our sector: data and privacy, product safety, consumer protection, the Digital Service Act (DSA), and Digital Market Act (DMA).

In our view, a simplification agenda means refraining from introducing new regulations unless absolutely necessary. We also urge policymakers to define a clear roadmap with a commitment to bold action, ensuring meaningful and early follow-up to the current Digital Omnibus under negotiation. This follow-up should include the simplification proposals put forward in this paper that may not make it into the final legal text.

Data and Privacy

Ecommerce Europe welcomes the Digital Omnibus on the data acquis as a beneficial first step in addressing the need for regulatory simplification. However, we find that some of the following points could have been better reflected in the proposal and would highly encourage their inclusion in future simplification efforts.

- Reduce regulatory complexity by clarifying existing frameworks and fully aligning Article 5(3) ePrivacy Directive with the six legal basis under Article 6 of the General Data Protection Regulation (GDPR), in line with the Commission's Data Union Strategy[1], and contrary to the proposed new Article 88a GDPR. The ePrivacy Directive applies a basic "on/off" mechanism that relies solely on consent, unfit for today's highly complex technical environment. Bringing Article 5(3) of the ePrivacy Directive in line with the GDPR would make it possible to apply the GDPR's risk-based approach to cookies and similar tracking technologies, rather than relying exclusively on consent.

- Urge caution against the proposed new Article 88b GDPR which mandates browsers to introduce automated, machine-readable consent mechanisms, acting as a gateway to damaging centralised cookie management systems. We see such proposal as going beyond simplification and urge the European Commission to properly assess the far-reaching consequences through a proper impact assessment. Ecommerce Europe believes that the proposed Article 88b GDPR should simply not be part of a simplification law. Such centralisation would also concentrate consent management power in the hands of large browser providers, raising raising serious competition concerns and

[1] European Commission, Data Union Strategy, p.14 – link

undermining the ability of website operators to engage directly with their customers on data use and personalisation. Such an approach would narrow user choice, weaken the GDPR's standard of specific and granular consent, and risk concentrating market power in ways that conflict with the aims of the Digital Markets Act. Centralising consent signals within browsers also introduces security risks and would de facto elevate consent to the primary legal basis for data processing, even though the GDPR establishes several alternative lawful grounds.

The proposed exemption for media service providers under Article 88b(3) underscores a deeper concern with mandatory browser-based signals (the justification offered is not specific to the media sector). The same reasoning extends to any European service that lawfully relies on advertising revenue and on-site personalisation as part of its business model. It is important to recognise that a broad spectrum of legitimate businesses depend on the current framework to maintain viability and compete in an increasingly data-driven marketplace. Moreover, personalised content and services have evolved from value-added features into baseline user expectations. Limiting an exemption exclusively to media providers would therefore grant a sector-based advantage unrelated to the nature of the activity itself. To prevent market distortions and preserve technological neutrality, any rules should be designed to apply horizontally across industries rather than confined to a single category of providers.

- Incentivise and boost Privacy Enhancing Technologies (PETs) adoption and create technical standards for them. The European PET's landscape is technically complex, which creates a barrier to entry and invest in it, especially for SMEs. By legally acknowledging PETs, companies would be able to rely on a clear legal basis to invest in and use these technologies, ensuring legal stability and confirming that PETs are recognised and permitted at EU level. **Today, the ePrivacy Directive, and proposed Digital Omnibus, require explicit, opt-in user consent for various PETs that rely on processing or storage capabilities of the user's device. This situation places the development of PETs on the same legal ground as a tracking cookie which creates a major disincentive for business adoption**. We believe PETs would help to avoid cookie fatigue while providing security for the users. Rather than relying on excessive and often meaningless consent requests, a more meaningful, security-based approach enabled by PETs should be encouraged. In addition, we urge broader, more practical set of exemptions that reflect the realities of e-commerce and recommend exempting recognised PETs from consent requirement. We also encourage the European Commission to develop common, interoperable PET standards for PET development. This infrastructure should be founded upon open, interoperable web and app standards that are platform-agnostic in collaboration with standards bodies (like W3C) to build accessible and affordable PET-based services, moving away from proprietary 'walled garden' solutions to ensure a level playing field for all businesses. PETs must be deployable, accessible and available to all payer in the digital supply chains and must not become another dependency tool.

- We urge caution against a full reopening of the GDPR[2]. In that regard we welcome the targeted approach of the Digital Omnibus as we believe that changes should only be done without adding additional rules to an already overly complex legal framework. Where possible, we would

[2] Ecommerce Europe, letter urging for caution against a possible reopening of the GDPR – link

encourage Data Protection Authorities (DPAs) to issue EU-level guidelines rather than national ones, as the latter may not always align. This would ensure avoiding unnecessary fragmentation of the interpretation in EU law.

Product Safety

In the Digital Single Market, products and services are offered for sales online and offline seamlessly. For smooth transactions and optimal customer experience to be guaranteed, it is instrumental to create one set of rules that can be applied in an omnichannel context. Nowadays, because of parallel lawmaking concerning product conformity, on the one hand, and e-commerce (with an emphasis on online intermediary services), EU regulations targeting e-commerce for products derive from different policy areas. Those shaping the free movement of information society services (e.g., e-Commerce Directive, TRIS Directive), and later the platform economy (e.g., DSA), as well as the EU product *acquis* (including the General Product Safety Regulation). Although coherence between the two policy tracks has been pursued, notably by equating the sale of dangerous and non-compliant products to 'illegal content', some discrepancies remain. These are related to specificities in the market dynamics and distribution chains, as well as to differing policy logics.

To tackle these divergencies, Ecommerce Europe suggests the following actions:

- Focus on a coherent implementation of the General Product Safety Regulation (GPSR), aligned with the EU product acquis and legislation regulating online content. To ensure that consumers benefit from clear and understandable product safety information, the framework must provide technology- and format-neutral requirements for businesses to implement. It is also crucial to stick to the concept of 'essential requirements', to prevent information overload for consumers, and to ensure harmonisation across Member States and product groups wherever possible. These key safeguards might be compromised if the 'e-vulnerability' of consumers were to be addressed under the GPSR, as this risks creating overlaps with existing consumer protection rules, such as the European Accessibility Act. Defining it as a universal concept to be applied to anyone buying online would have far-reaching consequences for the impact assessment of a product's safety. It would impose disproportionate burdens on businesses when displaying safety information online and would negate the benefits of enhanced protection for certain social categories who currently benefit from targeted measures aimed at reducing their vulnerability.
- Opt for the policy scenario of 'reshoring' the revised New Legislative Framework Regulation (NLF) and Market Surveillance Regulation (MSR) under a European Product Act (EPA). This would allow for more coherence in horizontal rules applicable to a large pool of products and ensure continuity between compliance and enforcement (and resources earmarked by companies and authorities to fulfil their respective tasks). Moreover, given the strong focus on digital compliance tools and e-commerce in the current reviews of the NLF and MSR, the EPA would enable an accrued uptake of digitalisation and e-commerce in the framework.
- Exploit the potential of the Digital Product Passport (DPP) and similar digital compliance tools to facilitate overall compliance and enhanced enforcement. However, costs associated with the digitalisation of product information should be assessed and mitigated. Such costs can arise owing

to the digitalisation of product compliance documentation, which already exists in physical format, and/or due to the very the roll-out or maintenance of digital compliance tools.

- Take advantage of the simplification opportunities offered by the DPP, which can function as "one source of truth" for product compliance across EU legislation, reducing parallel documentation requirements. The DPP must avoid introducing provisions that seem unnecessary to fulfil the policy goal and/or are overly burdensome, for instance, because they are not tailored to businesses' resources and technical capabilities (e.g., it is impossible to produce and display DPPs for online sales at a granularity deeper than model-level, or impractical to maintain DPP back-up copies for high-volume, seasonal, or short-lifecycle products such as clothing or consumer goods). Additionally, to further prevent the duplication of information requirements and thus ensure that the DPP-relevant content is usable and transferable, including in the context of the circular economy, harmonised standards for a uniform data collection, processing and language are needed.
- Ensure that the DPP implementation does not create obligations in contradiction with existing legislation and follows a gradual roll-out. For example, it is necessary to clarify and ensure that the DPP obligations for economic operators and providers of online marketplaces remain coherent with the Digital Services Act, ensuring that the responsibilities and liabilities for the data and its verification do not get passed down to actors at the end of the value chain.
- A major challenge is the coordination and governance between different authorities both at the EU and the national level when it comes to the DPP use. The DPP is mentioned in multiple pieces of legislation – both horizontal and vertical, both in force and underway, reflecting its potential to serve several policy objectives (e.g., product compliance, increased sustainability and circularity, enhanced market surveillance and customs activities). In the face of fragmented competences and overlapping policy objectives, it is important to ensure that the new data-oriented and IT-intensive approach is shared and "owned" by all authorities involved.

Consumer Protection

Ecommerce Europe firmly believes that the legal framework pertaining to consumer protection is mature, comprehensive and capable of addressing the practices identified in the various reports issued in recent periods. We are convinced that the recurring problem is not a lack of rules, but the uneven and inconsistent enforcement of existing ones.

Policy efforts should therefore focus on strengthening implementation, increasing consumer confidence, and ensuring a predictable and coherent legal environment for businesses operating across the Single Market. The objective should be to make existing rules work better, not to multiply legislative acts.
In this context, we recommend prioritising the following:

- **Strengthen enforcement and coordination**, notably through the CPC Network, by harmonising guidance, improving cooperation, exchanging best practices and developing advanced digital enforcement tools.
- **Provide targeted, case-based guidance** to clarify existing provisions and support both businesses and authorities in their practical application.

- **Support businesses in scaling across the EU** by safeguarding a harmonised Single Market and preventing additional fragmentation through overlapping or inconsistent initiatives.
- **Ensure coherence across ongoing policy developments**, including the Digital Product Passport, the New Legislative Framework and Customs Union reform, so that instruments operate consistently and predictably.

- **Promote simplification and voluntary cooperation**, including structured dialogue with businesses to identify compliance challenges, encourage good practices and strengthen consumer awareness.

The current drive for creating more and more legislation risks deepening fragmentation, increasing compliance burdens, and creating further uncertainty for both enforcers and businesses. The Fitness Check, as well as the conclusions of the Draghi and Letta reports, point in the same direction: the Single Market needs a period of consolidation, not expansion, of its digital rulebook. The goal should be to make existing laws work better, not to create new ones that risk overlapping with what is already in place.

Digital Services Act

The DSA is relevant to tackle the sale and promotion of non-compliant goods, including counterfeit products. However, it is interesting to remark that product-related issues (such as a product causing allergic reactions, or products missing information, warnings, or including dangerous or non-compliant elements) were not always flagged via the framework of DSA notice and action mechanism, but rather via the EU Safety Gate (previously RAPEX), established under the framework of the GPSR. This shows complementarity between different policy fields and legislative instruments that tackle similar objectives but also signals possible overlaps between the DSA and the GPSR.

More generally, we stress the importance of maintaining alignment between the EU product *acquis* with the DSA – more specifically the provisions on the 'general monitoring obligation' prohibition and the conditional liability regime for online marketplaces. This is particularly key to ensure legal certainty for businesses populating the e-commerce sector, as well as effective and efficient enforcement in the Single (Digital) Market. Alongside acknowledging that such legal consistency was upheld with the entry into force of the GPSR, we plead that such approach be maintained throughout ongoing legislative initiatives, such as the revisions of the New Legislative Framework and the Market Surveillance Regulation, and the potential European Product Act.

Looking at the upcoming Article 91 Review of the DSA, the EC should assess whether the transparency reporting template can be simplified (focusing on outcomes rather than process metrics) and whether reporting frequency for non-VLOP platforms can be reduced to annual without undermining the transparency objectives the framework is designed to serve. Many of the categories are not relevant to retail and this should be a measurable deliverable in reducing burdens by 25% as promised by the Commission.

Furthermore, Article 24(5) of the DSA requires all online platforms (not just VLOPs) to submit content moderation decisions and statements of reasons to the Commission's database without undue delay, to allow for real-time updates "where technically possible and proportionate to the means of the online platform

in question". In practice, real-time API integration with the Commission's database requires significant technical infrastructure investment that is disproportionate for the vast majority of online platforms. The Commission previously identified approximately 10,000 online platforms operating in the EU. The number of platforms that have successfully integrated with the real-time reporting system remains a small fraction of this total, only 280 in fact, demonstrating that the current technical requirements are not proportionate to the means of most platforms in scope. The Digital Fitness Check should recommend that the Commission:

- Publish clear guidance confirming that batch submission on a regular schedule satisfies the "without undue delay" standard for non-VLOP platforms
- Provide a standardised, low-barrier submission interface that does not require bespoke API development
- Consider whether the real-time reporting obligation should be limited to VLOPs, with a simplified periodic submission mechanism for all other platforms

Digital Markets Act

The DMA was intended to ensure fair and open digital markets by putting in place clearly established criteria that would curtail the ability of gatekeepers to behave in a way that would reduce contestability. While it has been in force since October 2022 and applicable since March 2024, the tangible benefits remain limited. The process towards ensuring compliance has been slow, cumbersome and opaque. We encourage the European Commission to press forward with enforcement and ensure that a high level of compliance is achieved.

While the DMA sets out clear prohibitions and requirements, implementation is inconsistent and sometimes circumvented. Google and Apple continue to design interfaces that favour their own services, apply algorithmic pricing controls that restrict merchant flexibility, re-monetise steering through link-out fees and so on. It is evident that without stricter interpretation and clearer guidance, these obligations may not deliver on the expected outcomes.

The implementation of the DMA has been a very costly endeavour for both the regulators and companies, and the results so far have little to show for. In line with the ‘better regulation’ principles, the European Commission, or the European Court of Auditors, should undertake a thorough review of the DMA’s effectiveness. With effective enforcement, the DMA may be able to deliver on its promise of contestable and fair markets. Until then, its impact for business users and consumers will remain limited.

Lastly, we support the European Commission to continue to monitor all market players to identify and designate any new actors that may act as gatekeepers in their respective space.