

AIG Position Paper on the Digital Fairness Act Public Consultation

Executive Summary

AIG welcomes the Commission's focus on digital fairness but believes that the EU's existing consumer protection framework is comprehensive and fit for purpose. The primary challenge is a better enforcement coordination, practical guidance, and clarity about how overlapping legal instruments interact. Rather than introducing new binding legislation that would further fragment an already complex regulatory landscape, the Commission should prioritise strengthening enforcement mechanisms, providing practical guidance, and supporting self-regulatory initiatives.

The Unfair Commercial Practices Directive (UCPD) already comprehensively addresses dark patterns through its provisions on misleading and aggressive practices, as confirmed by the Commission's 2021 guidance.¹ All commonly identified dark patterns are covered by existing rules. The issue is enforcing existing rules. We recommend enhanced cross-border enforcement coordination through the Consumer Protection Cooperation (CPC) Network, EU-level guidance with practical case studies, regular coordinated enforcement sweeps, and technical capacity building for national authorities.

Proposed restrictions on personalised advertising risk creating unintended consequences whilst duplicating existing protections. The GDPR currently requires explicit consent for processing personal data for advertising purposes, making additional opt-in requirements redundant. The UCPD already prohibits exploitation of consumer vulnerabilities, whilst the GDPR prohibits processing special category data without explicit consent. The boundary between harmful exploitation and helpful personalisation is highly context-dependent, and blanket prohibitions risk capturing legitimate, consumer-beneficial personalisation.

Existing frameworks already provide substantial protection for minors. UCPD Annex I prohibits direct exhortations to children, the GDPR provides enhanced protections for children's data processing, and the AVMSD regulates commercial communications targeting children. A blanket prohibition on personalised advertising to minors would require intrusive age verification or a de facto ban on personalised advertising on platforms where minors are present.

Influencer marketing is regulated under the UCPD and AVMSD. The challenge is ensuring compliance, particularly among emerging content creators who often lack awareness of their obligations. This is fundamentally an education and capacity-building challenge, not a regulatory gap. We recommend industry professionalisation through education and training schemes like EASA's AdEthics², education-first approaches, targeted support for small actors, improved signposting and platform disclosure tools, and investment in monitoring technology for self-regulatory bodies. This addresses compliance failures more effectively than blunt regulatory instruments.

¹ [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229\(05\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05))

² <https://www.easa-alliance.org/adethics/>

It is worth noting that the advertising industry operates a mature self-regulatory framework that covers 97% of the EU's population. It handled 52,715 complaints in 2024, resolving 89% within a month,³ and operates at no direct cost to taxpayers. The Commission should recognise and support advertising self-regulatory mechanisms as valuable contributors to consumer protection that complement public enforcement through education and correction rather than sanctions.

The proliferation of digital instruments with different enforcement mechanisms creates genuine coordination challenges. The solution to digital fairness challenges lies not in creating additional regulatory layers, but in ensuring that our comprehensive existing framework is effectively enforced, clearly understood, and properly coordinated. This approach will deliver better consumer protection outcomes whilst maintaining the legal certainty and business sustainability essential for Europe's digital economy.

About AIG

The Advertising Information Group (AIG) (transparency number - 11220347045-31) is an informal European grouping of national advertising tripartites representing advertisers, advertising agencies and the media, along with several Brussels-based trade bodies. AIG advocates for a genuine Single Market in commercial communications and supports responsible advertising self-regulation in the EU. AIG is also an industry member of the European Advertising Standards Alliance (EASA).

About Advertising

Advertising plays a key role in the EU economy, contributing 4.6% of GDP, supporting SMEs, and driving growth in creative sectors. A study conducted by Deloitte showed that for every €1 spent on advertising it generated €7 for the wider European economy.⁴ Advertising also plays a key role in fostering brand competition, supporting product innovation while enabling a diverse and pluralistic media.

The key benefits of personalised advertising in Europe⁵:

- EU Business Growth: Secures €100 billion in additional sales for EU businesses.
- GDP Contribution: Contributes €25 billion to GDP and supports nearly 600,000 jobs.
- SME Empowerment: Generates €80 billion extra revenue for SMEs; 75% of SMEs say they would struggle to find customers without personalised advertising.
- Publisher Support: Publishers earn twice as much from personalised advertising compared to contextual advertising, generating an estimated €10 billion in revenue.
- Consumer Preference: 75% of European consumers prefer the current model of personalised advertising.

³ 2024 European Trends in Advertising Complaints, Copy Advice, and Pre-Clearance. EASA.
https://www.easa-alliance.org/wp-content/uploads/2025/09/EASA-Complaints-Annual-Report_2024_Final_Cover-2.pdf

⁴ Value of Advertising Report, Deloitte, <https://valueofadvertising.org/value-of-advertising/value-of-advertising-report/>

⁵ 'A personal touch', Implement Consulting, <https://implementconsultinggroup.com/article/personalised-advertising>

- Future AI Benefits: By 2030, generative AI-powered ads could create €250 billion in additional sales and support 1.4 million jobs in the EU.

Introduction

Consumer protection is central to the advertising industry's approach. Trust in advertising is commercially essential – it is key to the success of the brands and businesses dependent on advertising.⁶ This is why the industry operates a mature self-regulatory framework aligned with EU legislation.

The EU advertising self-regulatory system:

- Covers 97% of the EU population.
- Enforces at scale and with speed. For example, in 2024, it handled over 52,715 complaints, and resolved 89% within a month.⁷
- Is coordinated by the European Advertising Standards Alliance (EASA) and based on national codes aligned with the Unfair Commercial Practices Directive (UCPD) and the International Chamber of Commerce (ICC) Advertising and Marketing Code.
- Includes clear rules for influencer disclosures and proactive compliance initiatives such as training and certification programmes across several Member States.

EU consumers are among the most protected in the world, online and offline. The recent reinforcement of the EU's digital rulebook through the Digital Services Act (DSA), the Digital Markets Act (DMA), the Artificial Intelligence Act (AI Act), the Data Act, and the Audiovisual Media Services Directive (AVMSD) has created a comprehensive framework that complements EU consumer protection laws. However, the application of these instruments in conjunction with existing consumer protection legislation has created complexity and, in some areas, legal uncertainty.

The Commission's Digital Fairness Fitness Check Report,⁸ published in October 2024, evaluated three EU consumer law Directives and identified challenges in the digital environment, including concerns about dark patterns, unfair personalisation practices and misleading influencer marketing among others. The Fitness Check concluded that the estimated financial detriment to consumers is at least EUR 7.9 billion per year, whilst also highlighting enforcement gaps and market fragmentation.

This position paper responds to the Commission's public consultation on the Digital Fairness Act. Our response is guided by a central principle: the EU's existing consumer protection framework is comprehensive and fit for purpose. The primary challenge is not a lack of regulation, but rather a deficit in enforcement coordination, practical guidance, and clarity about how overlapping instruments interact. Rather than introducing new binding legislation that would further complicate an already fragmented regulatory landscape, the Commission should prioritise strengthening enforcement mechanisms, providing practical guidance, and supporting self-regulatory initiatives that complement public enforcement.

⁶ <https://adassoc.org.uk/our-work/the-value-of-trust-report/>

⁷ 2024 European Trends in Advertising Complaints, Copy Advice, and Pre-Clearance. EASA.
https://www.easa-alliance.org/wp-content/uploads/2025/09/EASA-Complaints-Annual-Report_2024_Final_Cover-2.pdf

⁸ https://commission.europa.eu/publications/study-support-fitness-check-eu-consumer-law-digital-fairness-and-report-application-modernisation_en

This position paper focuses on those areas of the Digital Fairness Act consultation where AIG has specific expertise in advertising and commercial communications regulation. We address dark patterns (Section 1), personalisation practices (Section 4), influencer marketing (Section 5), and simplification measures (Section 8), corresponding to the consultation structure. We do not take positions on addictive design features (Section 2), video game-specific features (Section 3), pricing practices (Section 6), or digital contracts (Section 7), as these fall outside our core area of expertise.

Dark Patterns (Section 1)

Strengthened Enforcement, Not New Legislation

The existing Unfair Commercial Practices Directive (UCPD) already provides comprehensive coverage of so-called dark patterns. The Commission's own guidance (2021/C 526/01)⁹ demonstrates that the UCPD's principle-based approach effectively addresses manipulative interface design through its provisions on misleading practices (Articles 6-7), aggressive practices including confirmshaming (Articles 8-9, specifically Article 9(d)), as well as the blacklist in Annex I – which expressly prohibits fake urgency (No. 7), bait-and-switch tactics (Nos. 5 and 6), and other common dark patterns.

All practices commonly identified as dark patterns – including click fatigue, false impressions of limited choice, nagging, pressuring through urgency claims, confirmshaming, sneaking items into baskets, features leading to different results than expected, ambiguous language, and presenting choices in a leading manner – are already addressed by existing UCPD provisions. The issue is not identification of problematic practices, but rather enforcement of existing rules.

Courts and regulators (e.g. ACM,¹⁰ UOKiK,¹¹ OLG Bamberg¹²) have shown that enforcement works in practice. Additional rules would not add value but create overlap.

Rather than introducing new binding legislation that would create overlaps with the DSA, GDPR, and AI Act, we advocate for strengthened enforcement of the existing UCPD framework through the following measures:

Enhanced Cross-Border Enforcement Coordination

The Consumer Protection Cooperation (CPC) Network should develop coordinated enforcement strategies and provide targeted guidance at the EU level. Given the pan-European nature of digital platforms, consistent enforcement across Member States is essential to avoid forum shopping and ensure Single Market effectiveness.

⁹ Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=oj:JOC_2021_526_R_0001

¹⁰ The Dutch Authority for Consumers and Markets (ACM) imposed a €1.125 million fine on Epic Games for using artificial time pressure and deceptive scarcity mechanisms in Fortnite's in-game store

¹¹ The Polish Competition and Consumer Protection Office (UOKiK) fined Amazon for misleading delivery countdowns, unclear contract formation rules, and hidden conditions for "guaranteed delivery" on Amazon.pl, relying on provisions transposing the UCPD into Polish law.

¹² See ruling of the Higher Regional Court (OLG) of Bamberg concerning the ticketing platform Eventim (OLG Bamberg, 5 February 2025, 3 U Kla 11/24 e).

EU-Level Enforcement Guidance

Building on the Commission's 2021 guidance on UCPD application to digital practices, the Commission should develop:

- Practical enforcement manuals with case studies demonstrating how specific dark patterns breach existing UCPD provisions.
- Interface design assessment tools for national authorities.
- A clear benchmark for what constitutes 'professional diligence' in interface design (Article 5 UCPD).

Proactive Monitoring and Sweep Exercises

We also recommend regular coordinated enforcement sweeps focusing on high-risk sectors and platforms where dark patterns are prevalent, similar to successful CPC actions in other areas, as this would demonstrate regulatory presence and deter non-compliance.

In addition, national enforcement bodies require resources and technical expertise to identify sophisticated dark patterns, including training on interface design psychology, manipulation techniques, and expertise in assessing algorithmic and personalised manipulation.

Transparency in Enforcement Outcomes

The Commission should publicise enforcement actions and decisions to establish clear precedents, educate businesses about compliance obligations, and deter violations—following the principle that visibility of enforcement is as important as the penalties themselves.

This approach leverages the UCPD's proven flexibility whilst addressing the practical enforcement gaps identified in the Digital Fairness Fitness Check. New legislation would risk fragmentation with overlapping instruments (DSA, GDPR, AI Act), increase compliance costs, and require years to implement – whilst the enforcement deficit could be addressed immediately using existing powers.

Unfair Personalisation Practices (Section 4)

No New Actions Required

We believe that no new EU actions are needed concerning personalised commercial practices. The existing regulatory framework adequately addresses concerns about unfair personalisation through multiple complementary instruments:

The UCPD's provisions on aggressive commercial practices (Articles 8-9) already prohibit practices that exploit consumer vulnerabilities. The Commission's 2021 UCPD guidance explicitly states that data-driven personalisation practices exploiting consumer vulnerabilities can constitute 'undue influence' under Articles 8-9, regardless of trader intention.

The General Data Protection Regulation (GDPR) provides comprehensive rules on the processing of personal data, including for profiling and automated decision-making. GDPR Articles 13-14 require transparency about the logic involved in profiling, whilst Article 22 provides specific protections regarding automated individual decision-making.

The Digital Services Act introduces additional obligations for online platforms, particularly Very Large Online Platforms (VLOPs), to assess and mitigate systemic risks related to their recommender systems and targeted advertising practices (DSA Articles 34-35).

Consumers often find personalised offers and content useful, and survey data consistently demonstrates consumer preference for relevant advertising over generic alternatives. The challenge is ensuring that personalisation practices respect fundamental rights and do not exploit vulnerabilities – a challenge adequately addressed by the existing framework, provided enforcement is effective.

Creating additional regulatory layers specifically addressing personalisation would risk contradicting or duplicating these existing provisions, creating legal uncertainty and increasing compliance complexity without proportionate benefit to consumer protection.

Personalised advertising proposals: risk of unintended consequences and regulatory overlap

The Commission has suggested several measures regarding personalised advertising, including enhanced opt-in/opt-out mechanisms, restrictions on vulnerability-based targeting, and prohibitions on advertising to minors. Whilst AIG shares concerns about manipulative practices, these proposals risk creating unintended consequences and duplicating existing protections.

Opt-in/opt-out for personalised advertising duplicates GDPR

The GDPR already requires explicit consent for processing personal data for advertising purposes (Article 6) and the ePrivacy Directive regulates cookies and tracking technologies. Adding consumer protection law requirements for opt-in/opt-out would:

- Create parallel consent regimes with potentially conflicting requirements (e.g., does GDPR consent satisfy consumer law opt-in?).
- Generate legal uncertainty for businesses about which standard applies.
- Confuse consumers with multiple consent requests for effectively the same purpose.
- Risk undermining GDPR's comprehensive data protection framework by fragmenting consent requirements across instruments.

Interestingly, the Commission's UCPD guidance already recognises this overlap, stating that "existing decisions by data protection authorities concerning a trader's compliance or non-compliance with data protection rules should be taken into account when assessing the overall fairness of the practice under the UCPD."

Rather than enhancing control, multiple overlapping consent requirements could lead to further 'consent fatigue', reducing the meaningfulness of all consent mechanisms.

Vulnerability-based restrictions are already covered and operationally problematic

The UCPD already prohibits exploitation of consumer vulnerabilities through its provisions on aggressive practices (Articles 8-9). The guidance explicitly states: "The use of information about the vulnerabilities of specific consumers or a group of consumers for commercial purposes is likely to have an effect on the consumers' transactional decision...such practices could amount to a form of manipulation in which the trader exercises 'undue influence.'"

It is worth highlighting here that GDPR Article 9 already prohibits processing special category data (including health, ethnicity, religion) without explicit consent and strict conditions. Additionally, GDPR recitals specifically highlight that children warrant specific protection in data processing.

Operational problems with new restrictions

The boundary between harmful exploitation and helpful personalisation is highly context-dependent. For example:

- Is showing budget-friendly products to consumers facing financial constraints exploitative or helpful?
- Is promoting mental health resources to someone showing signs of distress manipulative or supportive?
- Are age-appropriate product recommendations to older consumers discriminatory or sensible?

The UCPD's principle-based approach allows case-by-case assessment of whether practices "materially distort" consumer behaviour. Blanket prohibitions risk capturing legitimate, consumer-beneficial personalisation.

'Vulnerability' is situational and dynamic: The UCPD recognises that vulnerability is not static — consumers may be vulnerable in one context but not others. Operationalising this into technical advertising restrictions would require:

- Real-time determination of consumer vulnerability states
- Classification systems that may themselves raise privacy concerns
- Businesses to make subjective judgements about consumer mental/emotional states

Overly broad restrictions could force businesses to avoid any personalisation that acknowledges consumer circumstances, potentially resulting in less relevant, more annoying advertising, or pushing consumers toward products less suited to their actual needs and financial situations. To further illustrate this problem, consider the advertising and marketing of flowers. If a consumer is searching for flowers to purchase, are they buying them for:

- A loved one, i.e. member of the family, friend, partner or spouse?
- Themselves to enhance their mood or to liven up the home?
- A funeral to commemorate the loss of a loved one?

Prohibition on advertising to minors is over-broad and already addressed

UCPD Annex I No. 28 already prohibits "direct exhortations to children to buy advertised products or persuade their parents or other adults to buy advertised products for them." The GDPR provides enhanced protections for children's data processing. AVMSD regulates commercial communications on audiovisual media targeting children.

Operational problems with blanket prohibition

Would this prohibit:

- All personalised advertising on platforms where minors are present (effectively banning personalised advertising for mixed-age audiences)?
- Age-appropriate product advertising for products designed for young people (e.g., educational tools, age-appropriate books, school supplies)?
- Family-oriented advertising that happens to reach minors?

Effective implementation requires robust age verification, which raises privacy concerns and is technically challenging. Many online service providers cannot reliably determine user age, without the use of more intrusive measures, particularly for younger teenagers who may misrepresent their age.

The existing multi-layered framework (UCPD, GDPR, AVMSD) already provides substantial protection for minors. The Commission's own UCPD guidance includes specific examples of unlawful practices targeting children and teenagers with personalised manipulation.

Overly restrictive rules may push advertising for youth-oriented products entirely to non-personalised, broadcast formats that are less accountable and transparent, or to platforms operating outside EU jurisdiction.

Harmful Practices by Social Media Influencers (Section 5)

The Need for Non-Regulatory Measures

With the increasing importance of social media for consumer transactions, reports of problematic commercial practices by influencers have become more prominent. However, AIG believes that these challenges are best addressed through non-regulatory measures, particularly education and industry professionalisation, rather than new binding legislation.

Understanding Non-Compliance

Effective consumer protection requires a deep understanding of why non-compliance occurs. Many influencers lack awareness of their obligations, misunderstand them, or enter the field unintentionally—often through a single viral post. Other factors that might cause improper disclosure include fear of generating negative consumer and follower attitudes toward branded social media content, or in other words being seen as inauthentic or ‘having sold out’. We believe a more effective way of addressing these root causes is through further professionalisation of the industry and boosting education efforts. We argue that this would increase compliance more effectively than blunt regulatory instruments.

Industry Professionalisation and Training

AIG supports EU-level promotion of education and training schemes such as EASA’s AdEthics. This equips influencers with knowledge of disclosure obligations, signals credibility to consumers and brands, and addresses compliance failures stemming from lack of awareness rather than intentional deception.

Education-First Approach

Building on successful models in France, Germany, the Netherlands, Austria, and the UK’s Advertising Standards Authority (ASA), the EU should facilitate sharing of best practices and

develop platform-specific guidance and accessible resources. Evidence suggests this approach changes behaviour more effectively than punitive measures alone.

Targeted Support

Compliance issues also tend to occur when small brands collaborate with small influencers, where neither has sufficient expertise or knowledge regarding compliance. AIG advocates for simplified toolkits, helplines, and onboarding guidance specifically designed for emerging content creators and small businesses entering the influencer marketing space.

Addressing Systemic Barriers

Some influencers believe that standard disclosure formats like '#ad' cause algorithmic deprioritisation. This may warrant further research to determine whether this is true or not. In any case, platforms should improve the prominence and user-friendliness of built-in disclosure tools and signposting of relevant resources. Removing these potentially systemic obstacles to compliance is essential.

Investment in Monitoring Technology

Some self-regulatory bodies have been experimenting with machine-learning monitoring tools to detect non-compliance. Longer-term monitoring technology is crucial for meeting the scale challenge of influencers online, and it is important that self-regulatory bodies have the resources and technical capability to monitor this expanding industry.

Legal Framework

It is worth noting that influencer marketing is already regulated under the UCPD, with specific guidance provided in the Commission's 2021 Notice (Section 4.2.6). The UCPD requires clear disclosure of commercial intent, and this applies equally to influencers. Additionally, influencers who meet the criteria set out in Article 1(a)(i) and (g) of the AVMSD can qualify as on-demand audiovisual media services and are required to comply with specific requirements for the fairness and transparency of advertising.

The challenge is not a lack of regulation, but rather ensuring that those entering the influencer space – often inadvertently – understand and can comply with their existing obligations. This is fundamentally an education and capacity-building challenge, not a regulatory gap.

Simplification Measures (Section 8)

Support for Harmonisation Through Guidance

We support measures to simplify consumer laws that reduce regulatory burden for businesses whilst maintaining high consumer protection standards. However, we emphasise that simplification should be achieved through guidance and best practice sharing rather than new binding legislation.

Harmonising Commercial Communication Disclosure Requirements

AIG supports harmonising disclosure requirements for commercial communications across Member States. Currently, divergent national interpretations of UCPD information obligations

create unnecessary compliance complexity for businesses operating cross-border, particularly for digital advertising campaigns that reach multiple markets simultaneously.

Whilst maintaining high consumer protection standards, the Commission should clarify through guidance which specific information elements are truly essential for consumer protection versus those that create administrative burden without proportionate benefit. This would reduce fragmentation whilst ensuring consumers receive meaningful, digestible information rather than overwhelming legal text.

Importantly, such harmonisation should be delivered through Commission guidance and best practice sharing rather than new binding legislation. This approach would provide the necessary clarity for cross-border operations without adding another layer of regulatory complexity to an already crowded landscape.

Single Market Fragmentation

We note that fragmentation exists in the area of commercial practices by social media influencers, where divergent national interpretations of disclosure requirements create compliance challenges for content creators and brands operating across multiple Member States. However, as outlined in Section 5, this should be addressed through harmonised guidance developed in cooperation with self-regulatory bodies, rather than through prescriptive EU-level legislation.

The Challenge of Regulatory Overlap

The proliferation of digital instruments with different enforcement mechanisms creates genuine challenges for both consumer protection and business compliance. The DSA is enforced by Digital Services Coordinators; the DMA by the Commission; the UCPD by national consumer authorities; the AI Act by market surveillance authorities; and the GDPR by data protection authorities. This fragmentation creates risks of enforcement gaps where authorities defer to each other, inconsistent interpretation of similar concepts across instruments, and forum shopping by platforms about which regime applies.

The Digital Fairness Fitness Check Report identified fragmentation and enforcement inconsistency as key problems, recommending 'further action' to address coherence issues. However, the solution is coordination and clarification of existing instruments, not additional legislation. New binding rules would further complicate an already fragmented landscape.

Digital Services Act Article 25 and UCPD Interaction

We note the legal uncertainty created by DSA Article 25 exclusion of practices covered by the UCPD and GDPR. The European Parliament's own research service identifies this as a significant issue: whilst the DSA prohibits dark patterns, it excludes practices covered by the UCPD. Given the UCPD's broad scope covering all B2C commercial relations, the space left for applying the DSA prohibition is severely limited.

This raises the question: when a dark pattern on an online platform potentially violates both the UCPD and DSA, it remains unclear which legal framework takes precedence, which enforcement authority has jurisdiction, and what standard of assessment applies.

The Commission's own Digital Fairness Fitness Check Report raised concerns about this interaction and noted it 'creates legal uncertainty' and potentially hinders the enforcement of both the UCPD and DSA.

Rather than introducing new legislation, we suggest clarifying the relationship between DSA Article 25 and UCPD through joint guidance from DG JUST and DG CNECT, clear criteria for determining which instrument applies, and coordination protocols between Digital Services Coordinators and national consumer protection authorities.

AI Act and Manipulation Provisions

The AI Act prohibits 'subliminal techniques' and 'purposefully manipulative or deceptive techniques' (Articles 5(1)(a) and (b)) that could cause significant harm. However, unlike the UCPD, these terms require case-by-case interpretation and are not further defined.

We foresee a particular problem when AI-powered dark patterns (e.g., personalised manipulation based on consumer profiling) could fall under both the AI Act and UCPD. The AI Act's requirement to prove 'purposefully' manipulative intent differs from the UCPD standard, which does not require intention. Some AI-driven exploitation of vulnerabilities (e.g., emotion recognition) is classified as high-risk but not prohibited under the AI Act, whilst potentially constituting aggressive practices under UCPD Articles 8-9.

The Commission's 2021 UCPD guidance explicitly states that data-driven personalisation practices exploiting consumer vulnerabilities can constitute 'undue influence' under Articles 8-9, regardless of trader intention. The AI Act's narrower, intent-based approach creates inconsistency.

Therefore, we recommend developing coordinated enforcement guidance clarifying that UCPD's broader consumer protection standards take precedence for commercial practices; AI Act provisions apply to the technology layer, UCPD to the commercial practice layer; and both can apply cumulatively where appropriate.

AVMSD and Influencer Marketing

Video-sharing platforms have obligations under AVMSD Article 28b(3)(c) to ensure appropriate disclosure of commercial communications. However, the UCPD also requires both influencers and platforms to ensure transparency as part of professional diligence obligations.

This creates overlapping but potentially divergent obligations, particularly regarding which disclosure format satisfies both AVMSD and UCPD requirements, and whether platform compliance with AVMSD relieves them of UCPD professional diligence obligations.

To address this problem, we recommend issuing joint AVMSD-UCPD guidance on influencer marketing disclosure requirements to ensure consistent interpretation.

Cross-Cutting Enforcement Coordination Gaps

We recommend establishing a formal coordination mechanism (potentially within the CPC Network) bringing together enforcers from different regimes to agree on interpretative approaches to overlapping concepts (e.g., dark patterns, manipulation, vulnerability);

coordinate investigations involving multiple instruments; and develop joint enforcement priorities.

These interactions create genuine legal uncertainty that harms both consumer protection and business compliance. However, the solution is coordination and clarification of existing instruments, not additional legislation.

The Value of Self-Regulatory Mechanisms

The Digital Fairness Fitness Check Report acknowledged the high effectiveness of private enforcement mechanisms for ensuring consumer redress, thereby underscoring the value of self-regulatory networks, such as EASA and its member self-regulatory organisations, in protecting consumers. Given that the Letta Report also called for horizontal instruments such as “self-certification and fast-track procedures to deal with minor non-compliances”, the Commission should recognise and support the contribution of advertising self-regulatory mechanisms to consumer protection.

Self-regulatory bodies offer several advantages: they can respond more quickly to emerging issues than legislative processes; they can provide sector-specific expertise and practical guidance; they operate at no direct cost to taxpayers; and they can complement public enforcement by addressing minor non-compliances through education and correction rather than sanctions.

Protection of Minors

We support protecting minors through existing regulatory frameworks rather than introducing new rules. The UCPD already prohibits direct exhortations to children (Annex I, No. 28), whilst the AVMSD provides comprehensive protection for minors on audiovisual media services (Article 6a) and video-sharing platforms (Article 28b).

The key challenge is enforcement and education rather than regulatory gaps. We recommend:

Enhanced Regulatory Coordination – This is important for consumer protection and media regulatory authorities to ensure consistent interpretation and enforcement across instruments. The intersection of UCPD, AVMSD, and platform-specific obligations creates complexity that can only be addressed through coordinated enforcement approaches.

Industry-Led Initiatives – These can include age-appropriate disclosure guidance for influencers whose audiences include minors, and integration of child protection obligations into training schemes such as EASA’s AdEthics.¹³ Those creating content for or accessed by minors must understand their enhanced responsibilities under existing frameworks.

Tools and Clearer Signposting – Platforms should continue to signpost influencers and provide clear tools and guidance when their content reaches minor audiences. Video-sharing platforms have obligations under AVMSD Article 28b to protect minors from harmful content and commercial communications, and should provide content creators with the knowledge and tools necessary to comply with these obligations.

¹³ <https://www.easa-alliance.org/adethics/>

Media Literacy Programmes – These help young people recognise commercial content and develop critical evaluation skills. Whilst regulatory compliance is essential, empowering minors themselves to understand and critically assess commercial communications provides complementary protection.

As highlighted in our response on influencer marketing, professionalisation and education address compliance failures more effectively than additional regulatory layers. The priority should be ensuring that those creating content for or accessed by minors understand their existing obligations, rather than creating new rules that add complexity without improving outcomes.

Conclusion

The EU's existing consumer protection framework is comprehensive, principle-based, and capable of addressing digital fairness challenges when effectively enforced. The primary obstacle to consumer protection in the digital environment is not a lack of regulation, but rather fragmentation between overlapping instruments, insufficient enforcement capacity, and lack of practical guidance on how existing rules apply to digital contexts.

Our position throughout this consultation emphasises several consistent themes:

First, existing EU consumer law – particularly the UCPD – already addresses the practices identified in the Digital Fairness Fitness Check, including dark patterns, unfair personalisation, and misleading influencer marketing. The challenge is enforcement, not legal gaps.

Second, the proliferation of overlapping digital instruments (DSA, DMA, AI Act, AVMSD, GDPR) creates coordination challenges that new legislation would exacerbate rather than resolve. The priority should be clarifying how existing instruments interact and establishing effective coordination mechanisms between enforcement authorities.

Third, many compliance failures – particularly in influencer marketing – stem from lack of awareness rather than intentional deception. Education-first approaches, industry professionalisation, and self-regulatory initiatives address these challenges more effectively than blunt regulatory instruments.

Fourth, regulatory intervention should respect appropriate boundaries. Data protection authorities enforce the GDPR; competition authorities assess market dynamics; consumer protection authorities enforce the UCPD. Maintaining clear delineation of regulatory competence ensures effective oversight without overreach.

Fifth, businesses require the freedom to develop sustainable business models, provided these models comply with existing legal frameworks. One-size-fits-all solutions risk undermining the economic viability of digital services, with particular implications for media plurality and access to information.

Rather than introducing new binding legislation through a Digital Fairness Act, the Commission should prioritise:

- Strengthening enforcement coordination through the CPC Network and similar mechanisms.

- Providing practical guidance clarifying how existing instruments apply to digital contexts.
- Developing joint enforcement guidance addressing interactions between overlapping instruments.
- Building technical capacity within national enforcement authorities.
- Supporting and recognising the valuable role of self-regulatory mechanisms.

The solution to digital fairness challenges lies not in creating additional regulatory layers, but in ensuring that our comprehensive existing framework is effectively enforced, clearly understood, and properly coordinated. This approach will deliver better consumer protection outcomes whilst maintaining the legal certainty and business sustainability essential for Europe's digital economy.

Advertising Information Group

24 October 2025