Digital fairness: enforcement, not a new law

Executive summary

Europe already boasts one of the world's most comprehensive consumer protection frameworks, applying horizontally across all consumer-facing businesses. A new Digital Fairness Act would merely duplicate existing regulations, driven by the mistaken belief that 'tech companies' require special regulation.[1]

EU consumer law is principles based and designed to adapt to new challenges without constant legislative revision. Manipulative design, false urgency, addictive features, misleading advertising, pricing tricks, influencer marketing and subscription traps are all explicitly addressed by existing consumer, data protection and digital legislation. Where automation is involved, safeguards on transparency and human oversight are already guaranteed. This includes the Unfair Commercial Practices Directive (UCPD), the Consumer Rights Directive (CRD), the Unfair Contract Terms Directive (UCTD), the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR).[2]

Some of the new concepts floated in the European Commission's public consultation – such as a blanket 'fairness by design' duty, redefining the 'average consumer' – would create vague standards that upend settled principles of EU law. Proposals like reversing the burden of proof would encourage defensive over-compliance; similarly, mandatory age checks would be counterproductive at the very moment when DSA rules on age-appropriate design are just starting to be implemented.[3]

Simplification should be a central ambition, both in respect of the Digital Fairness Act's approach to existing law and in any new proposals.

There is no absence of rules: the problem lies in uneven enforcement. Rather than producing duplicative requirements that only burden compliant businesses, the EU should focus on strengthening enforcement of existing laws.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14622-Digital-Fairness-Act_en.

[2] Directive (EC) 2005/29, Directive (EU) 2011/83, Directive (EEC) 93/13, Regulation (EU) 2022/2065 and Regulation (EU) 2016/679, respectively.

[3] See DIGITALEUROPE, *Protecting children online: response to the draft guidance*, available at https://cdn.digitaleurope.org/uploads/2025/06/Protection-of-Minors_DIGITALEUROPE.pdf.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

Table of contents

Enforcement is critical

Europe must prioritise full enforcement of its existing consumer and digital laws before adding any new regulatory layers. The challenges identified in the European Commission's call for evidence and consultation, as well as in the digital fairness fitness check[4], stem not from gaps in the law, but from inconsistent and insufficient enforcement.

To address these shortcomings, national consumer protection authorities must be equipped with the financial, technological and human resources needed to monitor fast-moving markets, investigate infringements and take decisive action. Stronger coordination across authorities and borders is equally essential.

Rather than contemplating a new Digital Fairness Act, the Commission should present an updated enforcement strategy – improving coordination, resource allocation, information sharing and the use of technology in investigations. It should also recognise the role of public-private partnerships and promote greater cooperation with industry.

Enforcement should be supported by EU-level guidance, drawing on behavioural insights, to clarify expectations in areas such as online choice architecture and addictive design. Such guidance should be principles based, technologically neutral and regularly updated.

Authorities should be encouraged to make greater use of digital monitoring tools, to coordinate enforcement through the Consumer Protection Cooperation (CPC) Network and to prioritise systemic cases (such as interface design practices) over isolated incidents.

Mapping out existing rules

Europe already has a comprehensive body of consumer and digital laws capable of addressing harmful market practices, from manipulative design to misleading advertising. The focus should be on improving enforcement and raising awareness of existing rights. Stronger enforcement will have a deterrent effect whilst supporting Europe's competitiveness.

Interface design

Deceptive interface design

Deceptive interface design – including manipulative tactics such as sneaking baskets and confirm shaming – is already addressed under several existing legal frameworks.

The UCPD bans unfair business practices, including misleading and aggressive commercial tactics. Art. 5 UCPD bans deceptive practices, whilst Annex I lists prohibited manipulative commercial strategies, including deception, undue influence and psychological pressure.

The GDPR reinforces consumer protections through Art. 7, which mandates clear and informed consent mechanisms, and Art. 25, which requires privacy by design to safeguard user autonomy against manipulative uses of personal data. The European Data Protection Board has also issued dedicated

[4] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14622-Digital-Fairness-Act_en.

guidance to support enforcement against deceptive design patterns, particularly in the context of social media and online services.[5]

In addition, the DSA specifically targets 'dark patterns' on online platforms. Art. 25(1) prohibits interface designs that distort consumer choices through misleading wording, coercive prompts or pressure tactics like confirm shaming. In addition, Art. 34 requires very large online platforms and search engines to conduct systemic risk assessments and mitigate any risks stemming from the design or functioning of their services, including those related to algorithmic systems.

The AI Act further reinforces this framework.[6] Art. 5 prohibits AI systems that exploit vulnerabilities to materially distort behaviour, making manipulative or deceptive techniques already unlawful under existing EU law.

Other tactics such as click fatigue, leading choices or using double negatives to confuse users also fall under UCPD prohibitions. Enforcement, however, must be strengthened. To support consistent application, the Commission should provide targeted guidance drawing on behavioural research, clarify the interplay between the UCPD, GDPR, DSA and AI Act, and promote best practices through cooperation with industry, consumer organisations and national authorities.

False urgency claims

False urgency claims involve creating a deceptive sense of scarcity or time pressure to push consumers into making hasty decisions. This tactic typically relies on false countdown timers, or misleading 'low stock' or 'high demand' messages that do not reflect a product's real availability.

The UCPD already clearly prohibits false urgency claims. Art. 6 forbids misleading statements about a product's availability, whilst Annex I explicitly bans fabricated claims of limited stock or time-sensitive offers. Businesses found using false urgency tactics can face penalties, including fines and corrective measures such as mandatory clarifications.

The DSA complements these obligations by requiring transparent presentation of rankings and offers on online marketplaces, ensuring that information about availability or promotions cannot be distorted through manipulative design.

As with other interface-related practices, enforcement remains the key challenge. Authorities should coordinate actions through the CPC Network and prioritise systemic enforcement against recurring manipulative design practices across sectors, rather than focusing on isolated individual cases.

Spending and time-use limits

Whilst creating engaging and enjoyable products and services to win and maintain customers is an essential business practice in both the offline and online world, we support discussions on promoting healthy usage habits and remain open to exploring the best practices that empower users.

A wide range of tools are available at the device and app level for users to monitor their screen time or spending. These include screen time reminders, notification controls, autoplay settings and read receipt

[5] Guidelines 03/2022.

[6] Regulation (EU) 2024/1689.

options. Many services also allow users to filter or adjust the types of content they see, down to blocking individual words they may find unpleasant or irrelevant. In addition, default settings, age-appropriate configurations and parental controls provide effective safeguards to promote healthy digital engagement, particularly for children.

The existing regulatory framework – primarily the UCPD and the DSA – already addresses concerns related to addictive design. Under the DSA, very large online platforms must conduct risk assessments that explicitly consider risks to young people and adjust their services accordingly. The DSA also requires platforms to offer alternative recommender systems not based on profiling.[7] The DSA framework has already led to positive changes in platform design, demonstrating that existing regulation is both effective and adaptable.[8]

Concerns about so-called 'addictive' design must be approached with nuance. For minors, the DSA already provides a robust framework through Art, 28 guidelines, which require age-appropriate default settings and transparency obligations.[9] For adults, autonomy must remain central: features such as autoplay, infinite scroll or personalised recommendations can improve usability, accessibility and user experience, and are not inherently harmful.

Many companies already provide tools – at device, operating system and app level – to help consumers set boundaries, from screen-time reminders to parental controls. Legislating against abstract concepts such as 'attention-maximising' design would undermine innovation in service design. Proper implementation and enforcement of the existing DSA provisions, including practical guidance and cooperation between regulators and platforms, remain the most effective way forward.

Personalisation

Personalisation is a defining feature of digital services, enhancing relevance, user experience and resource efficiency. It also underpins media diversity and free content. At the same time, personalisation must be applied responsibly, especially where it involves vulnerable consumers or sensitive data.

The existing framework is already comprehensive. The GDPR, ePrivacy Directive, DSA, DMA and AI Act together impose strict rules on data use, transparency and user control. They include bans on the use of sensitive data and advertising to minors, obligations for recommender system transparency, data protection impact assessments (DPIAs) for high-risk practices and explicit prohibitions on manipulative AI techniques that exploit vulnerabilities.[10]

---

[7] Art. 38 DSA.

[8] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161.

[9] C(2025) 6826 final.

[10] Under the GDPR, lawful processing must respect strict principles (Arts. 5–6), transparency obligations (Arts. 12–13) and the right to object (Art. 21); it also requires DPIAs for high-risk personalisation (Art. 35). The ePrivacy Directive complements these obligations by regulating unsolicited communications (Art. 13 Directive (EC) 2002/58). The DSA introduces sector-specific restrictions: Art. 26 prohibits the use of sensitive personal data for targeted advertising, whilst Art. 28 prohibits targeting advertising to minors. The Commission is developing a code of practice for online advertising to strengthen compliance. Finally, the AI Act (Art. 5(1)(b)) prohibits manipulative AI techniques that exploit vulnerabilities.

Protecting vulnerable users is essential, but broad definitions of vulnerability or new horizontal restrictions are not needed. Proposals such as blanket opt-ins or bans on behavioural data risk damaging viable business models across multiple sectors, from media and retail to travel and journalism. Stronger and more coherent application of existing law across Member States is the most effective way to ensure fairness in personalisation.

Influencer marketing

The legal framework governing influencer marketing is comprehensive, but requires consistent enforcement. Under the UCPD, influencers are required to clearly disclose commercial relationships, ensuring transparency for consumers. The DSA and the AVMSD establish advertising standards for influencers.[11] Practices such as hidden advertising, misleading claims and the purchasing of fake likes or followers are explicitly prohibited.[12] Targeting children with advertising, or pressuring parents into making purchases on their children's behalf, is also expressly prohibited.

The 2021 UCPD guidance clarified the application of EU rules to influencers, requiring that paid promotions be clearly and directly labelled, without relying on vague hashtags or ambiguous language. The Commission's Influencer Legal Hub also provides practical support for compliance.[13] These initiatives demonstrate that the EU framework can address evolving practices, provided enforcement is prioritised and guidance continues to adapt.

Despite this regulatory foundation, concerns about undisclosed commercial content, misleading endorsements and the targeting of vulnerable groups persist. Rather than regulating these behaviours again, efforts should focus on strengthening enforcement mechanisms, fostering coordination across Member States and educating influencers and brands about existing obligations.

Clearer guidance and dedicated education campaigns, particularly for SMEs and individual creators, would improve compliance. Recognising industry initiatives such as the European Advertising Standards Alliance (EASA) AdEthics programme and tools like DiscloseMe could also help raise standards.[14]

Brands and agencies should also play a role in ensuring that influencers they work with respect legal obligations. Where minors are concerned, scrutiny should apply to sensitive categories such as promotions of unhealthy products or cosmetic interventions, but this can be managed through guidance under the existing framework.

[11] Art. 26(2) DSA requires platforms to provide users with a functionality to declare whether the content they upload contains commercial communications. Platforms must also ensure that other users are able to identify, in a clear and unambiguous manner and in real time, including through prominent markings, when content contains commercial communications. Similarly, Art. 28b(2) AVMSD applies specifically to video-sharing platforms. It requires providers to clearly inform users when programmes or user-generated videos contain commercial communications, and to provide uploaders with the means to declare whether their content includes commercial communications.

[12] Purchasing of fake likes and followers is a prohibited practice in point 22 of the UCPD blacklist.

[13] https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/influencer-legal-hub_en.

[14] See https://www.easa-alliance.org/adethics/ and https://www.easa-alliance.org/discloseme/, respectively.

Pricing practices

Consumers have a right to clear and accurate information about the total cost of a good or service before purchase. Existing consumer law, particularly the UCPD, already prohibits misleading or false information that could cause consumers to make choices they would not otherwise have made.

Practices such as drip pricing, unrealistic 'from' prices and unjustified reference pricing are already captured under this framework and clarified in Commission guidance. These provisions must be enforced more consistently across the single market, especially in sectors such as cross-border e-commerce and travel where violations remain too common.

Dynamic pricing, when implemented transparently, is a legitimate commercial strategy that balances supply and demand and fosters competition. The focus should not be on restricting pricing mechanisms, but on ensuring consumers understand when and how prices may vary. The Commission should begin with updated guidance to clarify how existing rules apply to newer pricing techniques.

Digital contracts

Subscription traps

Subscription traps arise when signing up for a digital service is easy, but unsubscribing is made deliberately complicated, requiring multiple steps, forms or even phone calls to deter users from cancelling.

EU consumer law fully applies to digital contracts and subscriptions concluded online. A one-size-fits-all 'cancellation button' mandate would be disproportionate and could raise cybersecurity risks.[15]

Since 2023, Art. 11a CRD requires businesses to provide a prominent and easily legible withdrawal function for all online contracts. Businesses must also acknowledge receipt of a consumer's withdrawal request.

Additionally, Art. 9(d) UCPD considers barriers to contract termination an aggressive commercial practice, providing a clear legal basis to address subscription traps. This principle is reinforced in the Commission's 2021 UCPD guidance, which stresses that unsubscribing must be as straightforward as subscribing.[16]

The DSA also strengthens protections against subscription traps in the context of online platforms. Art. 25(1) prohibits misleading interface designs that make termination more difficult than subscription, and empowers the Commission to issue additional guidance if needed.

Free trials

Concerns about free trials or auto-renewals are already addressed under the existing framework.

Free trials allow consumers to test products or services before committing to a purchase. They are a valuable, yet costly, marketing tool, particularly for small businesses seeking to attract new customers.

[15] Traders must be able to require secure authentication, such as logins, confirmation links or one-time passwords. Without these safeguards, automated bots or malicious actors could trigger illegitimate withdrawal requests, exposing both businesses and consumers to significant risk.

[16] 2021/C 526/01.

Free trials are already regulated under the CRD and the UCPD, which impose clear pre-contractual information requirements and have been further clarified through detailed guidance.[17] More restrictive rules would reduce the availability of free trials, forcing consumers to pay for services without the opportunity to try them first.

There is no need to separate trial periods from the main contract, as trials are, by definition, part of a broader paid agreement. When consumers sign up, businesses must ensure that consumers explicitly acknowledge their payment obligations and are clearly informed about trial terms, expiration dates and the moment when charges will apply.[18]

Requiring payment details at the outset serves several important purposes: it prevents abuse (such as repeated sign-ups under different identities), verifies customer age and reinforces consumer awareness of the payment obligation following the trial. Delaying the collection of payment information or introducing additional confirmation steps would distort the nature of a free trial and create the misleading impression of a completely free service.

AI-powered chatbots

AI-powered chatbots are increasingly used by businesses to communicate with consumers more efficiently and to provide targeted support. In many cases, businesses offer users the option to interact with a human upon request.

AI-powered chatbots are not automatically classified as high-risk under the AI Act. However, when deployed as part of a high-risk AI system, they fall within its scope. In such cases, Art. 14 mandates that systems be designed to allow effective human oversight throughout their operational lifecycle. Successful implementation and enforcement of the AI Act will be central to ensuring transparency and accountability in consumer interactions with AI systems, including addressing manipulative or deceptive practices.

In financial services, sector-specific rules already guarantee meaningful human intervention. The recent revision of the Distance Marketing of Financial Services Directive introduced a right for customers to request and obtain human intervention both at the pre-contractual stage and, in some cases, after the conclusion of a contract.[19] Similarly, Art. 18(8) of the revised Consumer Credit Directive provides for a right to human review where creditworthiness assessments rely on automated data processing.[20]

Additionally, Art 22 GDPR grants individuals the right to request human intervention in decisions based solely on automated processing, where such decisions produce legal or similarly significant effects.

Beyond these specific regulated contexts, imposing a horizontal ‘right to human contact’ in all chatbot interactions would fail to reflect the growing performance and reliability of automated tools, imposing costs on businesses without demonstrable consumer benefit. Well-designed automated systems can deliver high levels of customer satisfaction without the need for direct human involvement.

[17] Ibid.

[18] Art. 6 CRD.

[19] Introducing Art. 16(c) CRD.

[20] Directive (EU) 2023/2225.

Terms and conditions

Terms and conditions (T&Cs) should be transparent, accessible and easy for consumers to understand. Many businesses already invest significant resources in minimising the length of T&Cs and presenting them in a user-friendly format, including the use of plain language and clickable summaries to assist consumer navigation.

The real challenge is that much of the length and complexity stems from mandatory disclosures set out in EU law itself. Mandatory disclosures often cover the right of withdrawal, complaint procedures, dispute resolution mechanisms and data protection obligations, much of which is stipulated by law. Many of these obligations were designed for analogue formats, producing lengthy, legalistic texts that consumers rarely read and that are poorly adapted to mobile or voice interfaces. Instead of informing, they overwhelm users and hinder genuine engagement.

We therefore support efforts to simplify mandatory information requirements, including reducing repetitive disclosures in recurring transactions such as in-app purchases. Other outdated obligations, such as the requirement to provide a fax number or a paper withdrawal form, should be replaced with more relevant digital-era solutions like real-time chat support.

Summaries alone cannot replace full contracts and may even create liability if they diverge from the legally binding text. But modernising information duties and embracing digital-by-default communication would genuinely improve both consumer understanding and business compliance.

Digital products and video games

Transparency in digital product features, including in-game purchases and uncertainty-based rewards, is important. The commercial design of digital products must be non-exploitative; however, existing consumer protection rules – in particular the CRD and UCPD – already cover unlawful features such as misleading advertising or unfair contract terms. Enforcement should remain the first response.

In-game currencies and purchases are long-standing practices, already governed by European consumer law and industry self-regulation. The Digital Content Directive,[21] together with the PEGI Code of Conduct and widespread parental control tools, provide strong protections, including the ability to disable in-game transactions or set spending limits.[22]

Introducing prescriptive EU rules on video game design would duplicate existing obligations, disrupt established business models and undermine Europe's globally competitive games industry, particularly small studios in the free-to-play and mobile gaming sectors.

Regarding loot boxes and similar features with uncertainty-based rewards, approaches differ across Member States. We support greater transparency, for example through clear disclosure of the presence of loot boxes, enabling parents to make informed decisions. However, harmonisation should focus on guidance and consistent enforcement of existing law, not new prohibitions.

[21] Directive (EU) 2019/770.

[22] See https://pegi.info/pegi-code-of-conduct.

Misguided new concepts

The Commission's public consultation raises several sweeping ideas that are conceptually flawed and risk doing active harm.[23] Rather than clarifying the law, they would introduce legal uncertainty and increase litigation costs for Europe's 23 million companies, most of them SMEs. No such new horizontal obligations should be introduced.

A blanket 'fairness by design' requirement would be vague and subjective. Designing digital products involves trade-offs between accessibility, usability, functionality and personalisation. Such a duty would lack any clear benchmark for compliance, leaving businesses permanently exposed to subjective interpretations by regulators and courts.

Reopening the long-established definition of the 'average consumer' would equally undermine legal certainty. The concept has been consistently interpreted by the European Court of Justice for over two decades, balancing flexibility with protection for vulnerable groups.[24] Attempting to redefine it undermines consumer agency.

Reversing the burden of proof in consumer law cases would shift disproportionate compliance costs onto smaller firms, forcing them to document and defend every consumer-facing action. Such a change would encourage over-compliance, drive up costs and ultimately harm competitiveness.

Mandatory age assurance requirements would be counterproductive at a time when the DSA already sets out a risk-based framework for age-appropriate design and is in the process of being implemented. Adding a new horizontal obligation would introduce unnecessary uncertainty and overlap, whilst effective solutions are still being developed.

These proposals run directly counter to the EU's competitiveness and simplification agenda. Rather than creating sweeping new concepts and obligations, the focus should remain on enforcing existing rules consistently across the single market.

[23] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14622-Digital-Fairness-Act/public-consultation_en.

[24] In Case C-646/22, the Court of Justice confirmed that the 'average consumer' benchmark does not exclude the possibility that an individual's decision-making capacity may be impaired by constraints such as cognitive biases. This demonstrates the flexibility of the existing concept, which already allows behavioural insights to be considered without redefining the notion of the average consumer.

FOR MORE INFORMATION, PLEASE CONTACT:

Bianca Manelli

Manager for AI, Consumer, IP and Platforms Policy

bianca.manelli@digitaleurope.org / +32 499 71 28 89

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Annex – Legal mapping

Issue	Legal status
Deceptive interface design	The UCPD prohibits misleading and aggressive practices (Art. 5), with Annex I listing banned manipulative strategies, including deception and undue influence. The GDPR reinforces these protections by mandating clear consent (Art. 7) and privacy by design (Art. 25). The DSA bans 'dark patterns' on online platforms (Art. 25) and obliges very large online platforms to conduct systemic risk assessments and mitigate design-related risks (Art. 34). Enforcement is carried out by consumer and data protection authorities, the Commission, national digital services coordinators and the EDPB, which has issued guidance on deceptive design patterns on social media.
False urgency claims	The UCPD bans false urgency claims (Art. 6) and Annex I explicitly bans false claims about limited stock or time-sensitive offers when urgency is fabricated. Enforcement includes penalties such as fines and corrective advertising.
Spending and time-use limits	Tools at the app/device level (e.g. screen time controls, parental controls) are widely available to allow users to manage screen time and usage. The DSA addresses 'addictive design' by requiring risk assessments for large platforms (Art. 34), the provision of non-profiling recommender systems (Art. 38) and impact analysis on young users (Arts 28 and 34). UCPD provisions and evolving platform practices under the DSA already provide a solid regulatory base.
Subscription traps	Consumer law regulates digital subscriptions. The CRD (Art. 11a) mandates an easy withdrawal function. The UCPD (Art. 9(d)) prohibits making unsubscribing unnecessarily difficult and this is reinforced by the 2021 UCPD guidance. In addition, the DSA (Art. 25(1)) bans subscription traps on online platforms and empowers the Commission to issues further guidance if needed.
Free trials	Consumer law mandates explicit acknowledgment of payment obligations. The CRD (Art. 6) ensures clear information on trial terms, expiration dates and reminders. Free trials are also subject to UCPD guidance, which prevents abusive practices whilst allowing businesses to offer trials.
Personalised advertising	The GDPR regulates lawful data processing (Arts 5-6) and transparency (Arts 12-13), and provides a right to object to direct marketing (Art. 21). The DSA also bans targeted ads for children (Art. 28) and use of sensitive data (Art. 26) on online platforms. To further support implementation, the Commission is exploring a code of practice for online advertising.
Use of AI-powered chatbots	Under Art. 14 AI Act, chatbots used in high-risk AI systems must include human oversight. Additionally, for financial services, consumers have a right to a human interlocutor under Art.16(c) CRD and Art. 18(8) Consumer Credit Directive. In addition, the GDPR (Art. 22) provides a right to request human review where decisions based solely on automated processing, including profiling, produce legal effects.
Influencer marketing	The UCPD (Art. 6) mandates disclosure of commercial communications and Annex I (point 11) explicitly bans hidden advertising by influencers. The 2021 UCPD guidance requires clear labelling of paid promotions. The AVMSD (Art. 28(b)) reinforces ad transparency on video-sharing platforms and the DSA (Art. 30) requires clear labelling of advertisements and endorsements on online platforms.

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European businesses across multiple sectors, as well as citizens, to prosper through digital technologies. We wish Europe to grow, attract and sustain the world's best digital talent, investment and technology companies. Together with our members, we shape industry positions on all relevant policy matters, and contribute to their development and implementation. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations and scaleups which are global leaders in their fields, as well as national trade associations from more than 30 European countries.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20