DOT Europe contribution to the Digital Fairness Act public consultation

Introduction

DOT Europe appreciates the opportunity to contribute to the Digital Fairness Act (DFA) public consultation. We hope the evidence provided will support the European Commission's assessment as to whether any clear gaps exist and, if so, the appropriate and proportionate way to address these gaps. Should legislative intervention be considered necessary, it should address **clearly identified gaps** taking care to not conflate implementation gaps with legislative gaps, so to avoid duplicative or overlapping requirements.

This is particularly relevant following the last European Commission mandate, which adopted and implemented extensive legislation for online services, including updating the consumer acquis via the Modernisation Directive. Some of this legislation has entered into force only recently (DSA, the Modernisation Directive, as recognised in the European Commission's own assessment of its application) or has barely started to apply (AI Act). For instance, the Modernisation Directive has only applied since May 2022 and many Member States transposed the requirements much later; the DSA has only applied for all online services since February 2024 and to VLOPs/VLOSEs since August 2023. The evaluation period of the Digital Fairness Fitness Check (2017 – 2023) predates the majority of these interventions.

Furthermore, draft guidelines on Article 28 of the DSA (Minor protection) were published just days before this consultation was launched. The content of those guidelines significantly overlap with aspects of the DFA consultation and cannot be assessed for their effectiveness.

It is thus premature to draw conclusions about the effectiveness of these rules. It is also worth recalling the Council Conclusions on EU digital policy of May 2024, which underline that effective, coherent, and efficient implementation of recently adopted laws with the minimum administrative burden for public and private players should be the main priority for the current mandate.

These reservations about the evidence basis and ability to evaluate the status quo echo those of the Commission's own Regulatory Scrutiny Board.

Before delving into the specifics topics of the consultation, we would like to highlight a number of cross-cutting themes:

- The European Commission's recent assessment of the Modernisation Directive (June 2024) and the Consumer REFIT report (October 2024) noted that more work

is needed to ensure the consistent implementation and compliance with existing rules. Greater emphasis is needed on oversight and actions to aid traders' compliance.

- In particular, the report pointed out the need to prioritise effective oversight and, where needed, **enforcement to protect consumers**. Consumer harms arising from serious breaches are unlikely to be remedied by adding new provisions to a complex and relatively "fresh" legislative framework. In fact, adding yet more, potentially vague and far reaching laws will only increase legal uncertainty, making compliance and enforcement harder. The focus should rather be on exploring where the bottlenecks in effective compliance lie and supporting national authorities to better detect breaches and target their enforcement efforts.
- Additional focus should also be on providing support for traders to avoid inadvertent non-compliance, for example due to an absence of providing timely and actionable guidance on what is prohibited and what is permissible. Working together with traders to improve compliance and enforcement, endorsing best practices and self-regulatory initiatives would also be a helpful approach.
- Due to the complexity of the existing legislative framework, our members often experience different authorities looking at the same issue from a different perspective, within a Member State or across the EU. To address enforcement fragmentation and strengthen legal certainty for businesses the European Commission could explore ways to create the necessary conditions for different regulators active in issues cutting across consumer protection and other policy areas to work together in a structured manner (e.g., consumer protection authorities, privacy and competition regulators). Greater cooperation and coordination between regulators would ensure a more uniform and harmonised approach. For example, the Netherlands established in 2021 the Digital Supervisors Collaboration Platform, a formal mechanism that brings together several national supervisory authorities to ensure more effective, coherent, and efficient oversight of European digital laws. This could be an interesting model to look into more closely.
- Policy makers should **avoid rules that amount to specific prescriptive service / product design requirements**. Any new rules setting out precise specifications on exactly how a service should (or should not) look or how consumers should interact with it will be disproportionate, and harmful for innovation, as well as negatively impact the consumer experience and competition based on service differentiation. Consumer protection rules should continue to be outcome based with flexibility to ensure they can apply to the very diverse range of products and

services in the EU. Prescriptive approaches could also result in unnecessary engineering costs.

- Online service and content providers need a stable and proportionate regulatory regime that promotes certainty. To achieve this, **uniform application and interpretation of rules** across the Single Market would be necessary. We urge policy makers to avoid "gold-plating" of rules and ensure consistent interpretation across the 27 Member States.
- The European Commission should undertake an **analysis of how different overlapping pieces of legislation interact with one another** and consider a codification of relevant pieces of legislation (i.e., explain which set of rules takes precedence when similar topics are being regulated). The same practice should not be regulated multiple times by different regulators and under different legal frameworks.

DOT Europe firmly believes that the majority of issues under consideration in the consultation are already adequately addressed in existing rules. The majority of problems are not due to a lack of rules, but due to the complexity of the legal framework, as well as challenges around interpretation, implementation, supervision and enforcement.

Consultation process and improved policy-making

We regret that the structure of the DFA questionnaire does not allow for further input in cases where "no action" is selected. We would like to flag the most important of these identified shortcomings:

- Lack of option to justify "No action": There is no possibility for respondents to explain this particular choice, except in the additional submission to the consultation. This practice will not allow for accurate measurement of responses..
- Survey logic: Responses to the consultation trigger dependent questions. However, in most questions, for any choice except "No action", the options are the same and include specific actions. The only way to go beyond the presented options is by selecting "Other" but this is not immediately obvious.

DOT Europe remains committed to the process informing the Digital Fairness Act. We would like to use our response to provide further context in cases where this option is selected in our responses. We hope the European Commission's chosen approach to the questionnaire's format will still take further feedback into account.

Dark patterns

Harmful online choice architecture (harmful OCA, a term we consider more accurate than “dark patterns”) is already governed by a very extensive, complicated and interlocking regulatory regime. Relevant provisions already exist in the Unfair Commercial Practices Directive (UCPD, including Annex I covering specific practices that are banned in all circumstances), the Digital Services Act (DSA, with a specific focus on online platforms), the General Data Protection Regulation (GDPR, inter alia covering the giving and withdrawing of consent) and the AI Act (subliminal techniques). Those rules are broad and flexible enough to capture the perceived ‘harms’ the consultation refers to. Against the backdrop of this complicated regulatory framework, the focus should be on enforcing existing provisions. To be more precise:

- Article 5(1) AI Act expressly prohibits practices related to AI that deploy subliminal or purposefully manipulative or deceptive techniques, with the objective or effect of materially distorting the behaviour of a person by impairing the ability to make an informed decision and causing them to take a decision that they would not otherwise have taken.
- Article 25 DSA and the principle of safety by design expressly prohibits the design of an online interface "in a way that deceives or manipulates the recipients" of a service or "in a way that otherwise materially distorts or impairs" the ability of users "to make free and informed decisions".
- Article 6(1) UCPD explicitly calls out the "overall presentation" of a commercial practice being capable of constituting a misleading action if it deceives or is likely to deceive the average consumer, "even if the information is factually correct", and the practice causes or is likely to cause the average consumer to take a transactional decision they would not otherwise have taken in relation to the list of prescribed elements (e.g., the consumer's rights).
- Article 7(1) UCPD prohibits misleading omissions, which Article 7(2) states to expressly include ‘a trader ‘hiding or providing information in an ‘unclear, unintelligible, ambiguous or untimely manner.’

As a result, DOT Europe believes that no additional legislation is necessary. Outside of implementation, supervision and enforcement, which is a horizontal theme of our contribution, attention should focus on clarifying the interplay between the different legal instruments governing harmful OCA; the European Commission should also consider whether it is necessary to work on guidance on how to distinguish between legitimate business practices (persuasion) and ‘harmful ones’ (coercion, manipulation, deception’

and explicitly acknowledge that not all nudging falls within the scope of harmful OCA practices. Positive forms of nudging can enhance the consumer experience and should not be treated as coercive, manipulative, or deceptive. For example, design features that remind a buyer to double-check essential information they have entered or encouraging them to take a break are all legitimate, consumer-friendly practices. Similarly, availability messages can be helpful to the consumer when transparent and truthful.

Any such guidance should be led by a number of considerations:

- It is important to recognise that in an online context space is by definition constrained. Platforms have a strong understanding of the tools at their disposal for making information available to users, and understand which methods of conveying information perform the best. This allows them to tailor the information delivery to ensure users are making informed decisions, while also promoting the benefits of their products or services. This is also beneficial for consumers.
- Guidance as well as any laws should adequately consider how they can **encourage innovation and respect the fundamental freedom to conduct a business**, for example by avoiding overly prescriptive interpretations that veer into product or service design. Diversity of services, features and business models and the ability of companies to differentiate their services is necessary to allow a dynamic, innovative and competitive ecosystem. Moreover, it is necessary to note that **users value a seamless online experience,** sometimes aided by UI designs that make their decision making quicker or easier. Online service providers may nevertheless choose to introduce friction or guidance, such as added context of visual clues, where this could be helpful, for example when users should fully understand and consider the choice they are making to be more in control of their online experience (e.g., when defining privacy preferences or completing a transaction). Provided existing consumer laws are respected, this is a decision that should rest with the online service provider, who has an intimate knowledge of the nature of the service and user expectations and is best placed to determine the right places for moments for pause.
- **Consider consumer benefits** when a platform highlights key or important information that may impact the consumer's decision making but provides them a clear benefit. For example: highlighting sales or promotional information or the option to "confirm cancellation" as a way to make more prominent the option that respects the consumer's wish can amplify consumer choice. The vast majority of consumers enjoy the products and services they interact with and platforms should be given flexibility in how they market these benefits to the consumer. These promotions can still be fully aligned with fully informed decision making,

where they in fact can often be complimentary or delivered in the same context. Bolt-on, additive disclosures are not necessarily better for a consumer than a promotional surface that contains material terms and doesn't mislead or deceive, when measured as a whole.

- **Examine interplay with other pieces of legislation covering harmful OCA**: The definition of harmful OCA in the UCPD and its interactions with a large number of more specific legislation that covers specific harms or product scenarios (e.g., GDPR and harms to privacy, the AI Act and use of AI systems) needs to be clarified. DOT Europe believes that specific harms are best addressed in their respective legislation, with consumer law serving (as it currently does) as the safety net for whatever is not captured elsewhere.
- Finally, clear and coordinated guidance from the EC on the responsibilities of the diverse regulators enforcing 'dark patterns'-related legislation would ensure clarity and transparency amongst regulators and industry, enabling a consistent and aligned approach.

Addictive design

This is an issue that has featured prominently as part of the broader online safety debate and the consultation document provides its own definition of what constitutes an addictive design feature, without clarity on whether this is evidence-based. In addition, the European Commission seems to be considering far-reaching bans of certain practices, in what is a departure from the principle-based approach employed in consumer protection law.

The UCPD already prohibits aggressive practices for all traders if they significantly impair consumer freedom of choice through undue influence. Our platform members are already addressing the growing concern over digital well-being by offering tailored solutions, especially for minors, across different services and devices. They also have additional obligations to assess and mitigate societal risks such as protection of minors and mental well-being under the Digital Services Act (DSA), obligations that also cover addictive design (Article 28 guidelines already address a number of the same features referred to in the questionnaire and recital 83 explicitly mentions “behavioural addictions of recipients of the service”), including via provisions on profile-based recommender systems (which we have covered in our comments on unfair personalisation). The DSA also provides a number of tools for consumers to disable certain functionalities or tailor their online experience according to their preferences.

In addition, the AI Act prohibits the use of an AI system that exploits the vulnerabilities of a person due to their age, disability or specific social or economic situation, in a way that

is likely to cause them significant harm. For example, the European Commission's guidance on Article 5(1)(b) AI Act (prohibited practices) gives an example of using AI in a way that creates a system that is highly addictive to children. This shows that specific safeguards against design that can lead to overuse are also covered under the AI Act.

It is worth pointing out that a number of actions under consideration in the consultation are already available to consumers (for example choosing how recommendation-based content is presented or switching certain features off). In addition, discussing mandatory 'off by default' settings and bans on certain features does not consider that many of these are not inherently problematic and that banning or restricting them could have wide-reaching, unintended, consequences; when used responsibly, they serve legitimate user needs and are critical to the user experience. For example, recommendation-based content is highly relevant and indeed expected by consumers in a marketplace or music streaming context. If such features were set "off by default," consumers would actually have to spend more time searching for what they need - an outcome that undermines one of the main consumer benefits of a digital service and runs counter to the very objective of decreasing the time spent online. In the same context, recommendation systems may be helpful to facilitate the discovery of products from small businesses or promoting circular economy goals. Moreover, recommendations may also be beneficial in ensuring an age appropriate experience on certain platforms. Personalised recommendations may connect minors with high-quality content that matches their interests. This is particularly helpful as search tools can be challenging for younger children due to barriers like spelling and query formation. Personalised content can provide valuable support for youth, facilitating self-guided exploration and expanding access to information.

It is for this reason that any intervention should be risk-based and avoid unintentionally capturing beneficial practices. Blanket measures such as imposing arbitrary limits to service usage or forcing customers to opt-in would not work for all types of users or services. This is because different people use online services for different purposes: time spent on each service is inherently different due to the varying nature of services consumers use, as well as the user's circumstances at a given moment in time (weekdays, weekends, during holiday, during a long trip etc.) and level of maturity (13-year-olds are much different to 17-year-olds). Time spent online is a subjective and personal concept that does not allow for the drawing of accurate conclusions of overall service use; blanket bans will deprive users of exercising more control over their experience. Further, the actions under consideration in the consultation are specifically relevant to certain features present in the digital market now. Given the rapid pace of

technological development, it would be short-sighted to introduce targeted, prescriptive measures, that are not flexible enough to cater for what might come next.

Instead, policy makers should consider ways to empower consumers to make informed choices about how they use a service. Examples of such empowerment tools provided by our members include providing users control over their experience, such as screen time spent, ability to hide certain types of content or words that can be distressing, limit or mute notifications (e.g., disabling nighttime notifications for minors), choice of community and interaction, spending limits, , autoplay toggles, read receipts and parental controls (such as the option for parents to provide an age range for their children in a privacy-friendly way). These can help address possible risks of over-use, as can service-specific guides and resources to encourage empathy and positive interactions. Several of our members also have sets of robust policies which outline prohibited behaviours that can impact the overall wellbeing of the community and of individual users. It is important to note that these tools are being continually developed based on industry learning and research, as well as by supporting relevant academic research and working with various youth civil society groups.

The REFIT report of October 2024 avoided an examination of whether the current digital rulebook can address concerns identified in the report, asserting, without evidence, that the digital rulebook "only partially addresses some of the problematic practices examined in the Fitness Check". We would strongly support a full assessment to identify any gaps in regulation for services of concern, for instance in relation to specific harms, which are not and could not be addressed by enforcement of existing legislation. Addictive design features should be distinguished from legitimate product features that promote engagement with digital services Policymakers should adopt an evidence-based approach which prioritises identifying practices that are harmful and/or detrimental to consumers and avoids disrupting features that serve a public interest purpose such as surfacing diverse content in an online news service. Before creating new rules, the EU should first explore improvements under the existing framework, such as issuing guidelines or targeted amendments. Moreover, we invite policymakers to leverage successful industry practices and adopt a flexible, evidence- and risk-based approach. This empowers individual users with more options instead of defaulting to a restrictive, one-size-fits-all experience. No proposals should duplicate existing legislation and non-legislative action should be explored in the first instance. We invite the European Commission to consider the framing adopted in the DSA Art. 28 guidelines (features aimed at engagement that may lead to overuse) and look forward to engaging with the forthcoming inquiry on wellbeing.

DOT. europe
Digital • Online • Tech

Specific features in digital products, such as video games

In-app purchases and in-app currencies and engagement with other virtual items are long standing practices that are already governed by European consumer laws, such as the Digital Content Directive and Consumer Rights Directive. Companies are also subject to self-regulatory measures such as the PEGI Code of Conduct.

In-app purchases have led to positive developments in the gaming sector, and fuelled enhanced consumer choice as a result. While microtransactions remain optional, there are many existing parental control tools developed by industry that enable turning off specific features such as the ability to make purchases and put spending limits in place to give parents better control.

In-game virtual items, including currencies are a well-established and commonly used tool. They come with many benefits for the quality of the player experience, creating an immersive environment and driving the game's narrative forward by rewarding skill and strategy (e.g., resource management), as well as helping balance gameplay. They are valued by players, and provide vital revenue streams for digital content/ service providers, forming the cornerstone of the free-to-play model, which underpins the entire industry.

In-game currencies have been classified as digital content under the Consumer Rights Directive, the Digital Content Directive and as confirmed by case law[1], exchanges of in-game currencies for other virtual items in a game are not purchases. As such, these in-game items are not comparable to real world currencies and cannot be considered a payment method.

A legislative approach that recognised virtual currencies as purchases would require users to be presented with additional steps such as pre-contract information and right to withdrawal information at every step where they plan to redeem virtual currency for an in-game item. This is information they have already been presented with across their user experience (precontractual information and all other consumer protection steps required for real-money purchases when they first buy the virtual currency), but would now need to be provided several additional times, significantly interrupting their game experience without any additional consumer protection. The resulting disruption in consumer experience would go against user expectations and run counter to the goal of virtual currencies, which is to allow users to interact with the game in a more streamlined fashion.

[1] Regional Court for Civil Cases Vienna, judgement of 26 March 2025, 10 Cg 93/23d – 31.

Requiring providers to display a monetary value at all times and/or maintaining an exchange rate system would create the misconception that the in-game content has actual financial value and can be exchanged for real money. This is especially true for in-game virtual currencies which take place in a closed loop, without the possibility to "cash out". Moreover, many games also allow the consumer the possibility to earn in-game currencies through the course of playing the game, for free. Such displays of monetary value would thus be misleading to consumers.

We must also point out that features such as in-game currencies cannot simply be removed from a game or service. They are complex mechanisms that are integrated into the design and switching them on or off would require material investment in design, including creating multiple versions of the service or content exclusively for the EU market, in turn increasing required investment and complexity in operation. For many, such a requirement would not be possible to implement in practice or from an economic perspective, threatening availability in the EU market.

It is important to note that the industry has taken a number of measures to enhance consumer protection in this space. It is industry practice to keep commercial transactions in a clearly distinguishable "marketplace" or "in-game shop", following the approach recommended by the Office of Fair Trading (OFT), now CMA, in the UK from 2014, which the industry worked to adopt, and which was subsequently referenced by the European Commission as good practice[2]. Moreover, in-game purchases are subject to multiple safeguards at the place where the commercial transaction takes place. This helps users understand the commercial context of their spending decisions as they occur away from the service or digital content they are engaged in.. The industry has also introduced additional safeguards, such as tools to manage, limit or block purchases via parental controls as well as friendly refund policies. It has updated the PEGI Code of Conduct rules for purchasable in-game content, which now includes obligations on transparency in transactions, in-game currencies, paid random items and measures against skin gambling. Finally, the industry has recently put forward a set of proposals to address the concerns outlined in the Fitness Check and the CPC Network 'Key Principles on Virtual In-game Currencies'.

However, despite all those initiatives, and like in other sectors, some companies have engaged in questionable practices at the expense of the rest of the industry. It is

[2] Common Position of the national consumer enforcement authorities on consumer protection in games apps from December 2013 https://ec.europa.eu/commission/presscorner/detail/en/ip_14_847

important to have better enforcement against such rogue players, and to encourage them to follow recognised industry standards

Introducing prescriptive rules such as a ban on in-game currencies would upend established business practices and models, disrupt player experiences, create duplication of laws, and have damaging effects on the competitiveness of a leading industry in Europe. Many European game companies and studios, primarily made up of SMEs and start-ups, rely on in-app purchases to grow, particularly in the free-to-play and mobile game environment. Any rules as part of the DFA should also not disrupt the user's experience with extensive information requirements and contractual information for each microtransaction. We would encourage prioritisation of a constructive dialogue with the industry to address any issues as the current concerns can be fully addressed through existing EU Consumer Acquis and in combination with self- and co-regulation.

Unfair personalisation practices

The aspects of personalisation covered in the DFA questionnaire are already comprehensively governed by a complex regulatory framework, which means that no additional legislative action is needed.

Recommender systems and personalised ads are governed by the UCPD, the GDPR, the ePrivacy Directive, and the DSA, including specific provisions on personalised ads. Provisions include bans on targeted ads for children and use of sensitive data and the right to experience non-profile-based recommender systems. Legal texts touching on aspects of advertising also exist in the UCPD, CRD (requirement to disclose personalised pricing), Regulation on transparency and targeting of political advertising, Platform to Business Regulation, DSA Article 28 guidelines and AI Act. Potential concerns related to the implementation of personalised pricing are already addressed through the UCPD, GDPR and Price Indications Directive. This list is not exhaustive but is indicative of a complex and extensive regulatory framework already in place to safeguard consumers. This framework enables users to make their own informed choices on what types of services they want to receive and consumers already have robust choices around what data can be used. As such, additional regulation would not provide any meaningful benefit to consumers. Both the recent revamp of the consumer acquis (via the Modernisation Directive) and the DSA have already put in place substantial rights for users of online services, including:

- Transparency on the main sorting parameters used when presenting content.
- The relative importance of the sorting parameters used.
- Options for service recipients to modify or influence the parameters.

- Allow the recipient of the service to select and to modify at any time their preferred sorting option.
- VLOPs / VLOSEs having to provide a recommender system option that is not based on profiling.
- A requirement for VLOPs/VLOSEs to test and adapt recommender systems as part of risk mitigation measures.
- Clarification that "free" services accessed in exchange for viewing ads (providing personal data) are also considered transactions.
- Clearly marking paid for content and disclosing advertiser and targeting criteria for advertisements. Article 26 DSA requires that providers of online platforms showing ads should ensure that the recipients of the service are able to identify meaningful information directly and easily accessible about the main parameters used to determine the recipient to whom the advertisement is presented. Further, Articles 26(3) and 28(2) DSA implement a prohibition to present personalised advertising based on profiling using personal data towards minors and even towards all users if special categories of personal data are used.
- AI techniques that facilitate unlawful personalisation are also covered by existing prohibitions. Article 5(1)(b) AI Act prohibits AI systems that exploit vulnerabilities of an individual due to a range of protected characteristics with the objective of materially distorting the behaviour of that person in a manner that causes significant harm. The Commission's guidance on that prohibition gives an example of a game that uses AI to personalise unpredictable rewards in order to be highly addictive to children.
- At a more macro level, risks linked to personalisation, such as that algorithms may perpetuate biases and discrimination are addressed in the DSA as well as the GDPR.
- The GDPR applies horizontally to all data subjects and thereby all consumers whose personal data is processed to facilitate personalised advertising. The GDPR also restricts the processing of sensitive personal data and through its fairness principle (Art. 5(1)) ensures that data processing activities based on personalisation, including advertising, do not lead to unfair outcomes. Consequently, because of its wide, open and future-proof nature, the GDPR already addresses the practices that the DFA would seek to address under the exploitation of consumers' vulnerabilities to personalise commercial offers.

The impact of these provisions is not easy to measure, given how recently many of them have entered into force (and the fact that the Modernisation Directive has been in force in Member States only for about two years). The Commission should therefore consider phasing next steps so that further assessments can be done at the right time, with sufficient experience and data. It is worth adding here that the European Commission's

own assessment of the Modernisation Directive highlighted the lack of evidence due to the short period of application, which made the drawing of safe conclusions challenging[3].

Personalisation brings value to consumers and helps them effectively navigate vast quantities of online content, it is also an essential tool for online services to create safer online environments, particularly for younger users, as well as enhance fraud prevention (distinguish legitimate traffic from fraudulent activity).

It is also crucial to recognise that personalised advertising is a vital economic enabler for the European economy and for SMEs. By tailoring efforts to individual customer behaviours, businesses can effectively reach those consumers most likely to be receptive. This enhanced efficiency ensures that every marketing euro is spent wisely, allowing for a more strategic allocation of resources. It currently secures €100 billion in additional sales for EU businesses, contributes over €25 billion to the EU's GDP, and supports nearly 600,000 jobs. This is projected to more than double by 2030 to €250 billion in sales and 1.4 million jobs due to AI technologies.[4]

From the consumer perspective, the benefits of personalised advertising are about relevance and convenience. Instead of being bombarded with generic, irrelevant ads for products and services they have no interest in, consumers receive marketing messages that are tailored to their needs and preferences. This creates a much more efficient and less intrusive browsing experience.

Consumer attitudes to personalisation should also be measured using a robust methodology; it is worth noting here that the October 2024 REFIT report showed that the share of consumers who did not perceive any benefits from personalisation was a minority, ranging from 24% for ads, to 25% for ranking, and 32% for pricing (p. 162).

Any proven consumer issues related to digital advertising should be carefully assessed under the existing EU regulatory framework, and if needed during a review of the ePrivacy framework, rather than under the DFA.

Finally, while the need to protect vulnerable users is paramount, the DFA should avoid broad and subjective concepts of “vulnerability” (e.g., “emotional distress”) as this will create further legal uncertainty and hinder both compliance and enforcement. Any restrictions should focus on clear, objective categories of data. The introduction of unclear or subjective criteria, such as ‘negative mental states’, risks making restrictions unworkable, particularly for complex systems that require automation like advertising,

[3] Report as regards the better enforcement and modernisation of Union consumer protection rules, p. 34
[4] Implement Consulting, “Personal Touch”, May 2025

which processes thousands of ads per millisecond. Increased uncertainty may lead to over-enforcement, directly impacting the businesses that rely on those advertisements to thrive, and small and medium businesses in particular. A focus on clear, actionable and objective categories of data is essential to foster a competitive digital economy.

Harmful practices by social media influencers

There is already a comprehensive legislative framework that is relevant for influencers, brands and the platforms on which their content appears: The DSA (Article 26), AVMSD (Article 9(1) and Article 28b), the Unfair Commercial Practices Directive (Article 6(1), 7(2) and Annex 1), the Unfair Contract Terms Directive, the Consumer Rights Directive, the Digital Content Directive, the Consumer Sales Directive all apply. They include provisions covering the clear and prominent disclosure of commercial communications, bans on hidden promotions and transparency requirements, including on the labelling of posts, incentivised content and endorsements. They offer tools to tackle identified concerns related to influencers and the platforms their content appears on, including a number of options identified in the DFA consultation (e.g., prominent disclosure of advertising). As a result, no further rules are needed. However, the Commission should make clear that traders choosing to use influencers to endorse their products in paid-for adverts are already subject to EU rules around the content and placement of such adverts and this will be out of scope of any DFA proposals.

DOT Europe believes that education initiatives specifically for content creators and the brands they partner with that focus on applicable rules would be more effective than the introduction of new rules. The European Commission's Influencer Legal Hub is a great resource providing clarity on applicable rules; as an additional action, the European Commission should consider partnering with influencers and their representatives to increase the reach and user-friendliness of this resource. Moreover, self-regulation and the adoption of best practices by influencers and the brands they partner with can complement existing legislation, as this effort is most impactful when platforms and brands also take proactive steps to support compliance. Joint responsibility fosters a culture of accountability amongst influencers and brands and makes it easier to address specific challenges as they arise given the evolving nature in this space. To this end, an ongoing dialogue between policymakers, influencers, online platforms and other stakeholders is key to ensuring that regulatory frameworks are informed by practical insights and experiences.

As a final comment, flexibility to accommodate diverse platforms is essential. Different platforms and influencers have varying operational models and audiences. Flexible rules ensure that one-size-fits-all approaches do not hinder the unique aspects of different

platforms to the detriment of consumers and the influencer economy. The existing EU framework governing influencer marketing currently allows for this.

Unfair marketing related to pricing

Similarly to previous comments, we note that existing legislation protects consumers from misleading and unfair practices relating to pricing. CRD, PID, UCPD require traders to communicate the total final price to the consumer at the moment of sale. At the same time, it should be understood that there are cases where certain charges are not accessible or calculable upfront, and that consumers may make decisions through their ordering/booking process that could impact the final costs. Overall, consumers benefit most from accurate pricing at the point where it can be reasonably calculated. A flexible approach that allows displaying a clear base product price exclusive of delivery or extras, but identifying the existing of such charges and then prominently shows the total price at the basket stage, ensures both transparency and usability. Imposing overly rigid requirements would risk information overload and further consumer confusion, in addition to veering into product design without any clear consumer benefit.

Variable pricing can arise for many valid and legitimate reasons, including personalisation / customisation, volume discounts, new regulatory costs or buyer-driven choices such as shipping speed. Reference pricing should therefore be accurate but flexible enough to reflect that prices are not static. This flexibility is especially important in marketing contexts where consumers are guided toward affordable choices (e.g., “stemware under 50 Euros” or “Mother’s Day jewelry starting at 30 Euros”).

In addition, it is critical that the European Commission clarifies the distinction between marketplace obligations and seller obligations. Marketplaces facilitate transactions between buyers and independent sellers, but pricing and marketing tactics are determined by the sellers themselves. Purely two-sided marketplaces without their own stock or fulfillment infrastructure should not be held to the same obligations as vertically integrated retailers. Clear guidance on this distinction would ensure proportionality and prevent undue burdens on marketplaces.

Furthermore, regarding drip pricing, “headline price” requirements should be aligned with the consumer’s actual purchasing journey. The final price a consumer pays, including all mandatory charges, typically depends on the contents of the full basket - which can only be calculated once the consumer has made all relevant selections. The delivery address for a gift purchase may not be known until checkout, and delivery or service fees are highly dependent on destination, weight, and delivery speed. Such fees

should only need to be displayed once the basket has been calculated, ensuring that the consumer sees a clear, accurate and complete total price at the basket level.

When it comes to dynamic pricing, a clear distinction should be made between different forms of dynamic pricing and their application in different industries and business models. It is also crucial to keep in mind that competition on price is one form of legitimate and desirable form of competition that leads to price benefits for consumers.

In summary, the existing EU framework—notably the UCPD and CRD—is sufficient to protect consumers from misleading pricing practices. The challenges identified are not due to legislative gaps, but a need for stronger, consistent enforcement. Therefore, we urge the Commission to refrain from introducing new, duplicative legislation. Any outstanding ambiguities or new market developments can be addressed through targeted clarifications, which is the correct and proportionate tool to ensure legal certainty.

Issues with digital contracts

Online contracts, such as subscriptions, are covered in articles 7 and 9 of the Unfair Commercial Practices Directive (UCPD) and the corresponding 2021 guidance, which already specifies that cancellation should be as easy as signing up. The rules are further complemented by the Consumers Rights Directive (CRD), which protects consumers against User Interface designs that could lead them to place orders without clicking on a properly labelled button and requires traders to provide clear and prominent information on duration and automatic renewals. Moreover, DSA Article 25.3(c) considers "making the procedure for terminating a service more difficult than subscribing to it" a dark pattern. This comprehensive legal framework highlights the existing level of complexity and should inform the Commission's assessment about whether additional rules are justified. There should be no new overlap with existing systems, and appropriate exemptions for contracts covered by sectoral rules such as contracts that fall within scope of European Electronic Communications Code rules.

DOT Europe believes that any difficulties regarding subscriptions can in large part be alleviated by better implementation and oversight of the existing and comprehensive transparency and information simplification provisions, which provide clarity for consumers.

- **Subscription cancellation:** There are currently myriad online services that use subscriptions in different ways and for different types of products and services. Rules should remain flexible and principles-based and avoid prescribing specific solutions that may not work for some companies or consumers or may require

changes in well-functioning, existing systems. A good example of principles-based rules is the logic that cancelling a subscription should be as easy as signing up to one (as set out in the Commission's guidance on the UCPD), but without prescribing in hard law how this should work in practice. In addition, for security reasons, cancellation processes such as a "single cancellation button" that do not require customers to log into their accounts and confirm their identity would be legally unworkable and expose consumers to considerable risk. Logging in is not considered an unnecessary burden for consumers but rather a necessary measure to ensure account integrity, prevent abuse and ensure the relevant individual gives the instruction to take such a significant step; consumers may also be in a constantly logged on environment (like a store), while sometimes they may not be (or be on a different device). In addition, consumers in the online world already benefit from sufficient means to contact traders in case of any queries related to their contracts. Many traders provide customer support via phone and email in case of contract-related issues and offer extensive information on cancellation options online.

    - As an additional point specifically for services providing digital content for which current exemptions to the right of withdrawal exist, we would ask that this is strengthened / made more explicit by the DFA. These services incur costs (e.g., copyright royalties), for any content streamed after the point of purchase, so it would be unfair to place any legal obligation on them to refund in full consumers who have already used the service / accessed content.

- **Trials:** Under existing rules, customers must receive transparent and clear information in case subscriptions automatically continue after the trial period comes to an end, and have easy methods to cancel if they do not want to continue. Companies sometimes request payment information for trials to avoid misuse (e.g., signing up multiple times for trials, or for age verification or fraud prevention reasons). The user consciously enters into a paid subscription with the full protection of pre-contractual information, transparent pricing, "buy" buttons, transaction receipt and 14-day withdrawal right whereby the trial is usually a mere suspension of the payment obligation for a period of time. Traders have more opportunities to make value propositions to users when they can offer free trials where there is an easy and seamless way for satisfied consumers to automatically continue their subscription after the trial has ended. Without the opportunity to offer free trials without a second payment process, more developers will have to choose to either offer advertising based or paid services. There is also the added risk of service disruption or even loss if consumers forget to consent/miss the

process, as well as potential issues for consumers in circumstances where tenure of subscription can lead to additional benefits, which consumers enjoy receiving.

- **Auto-renewals:** Many services already remind consumers about subscription renewals and before free trials are converted into paid subscriptions with cancellation/opt out options for convenience. Consumers are also informed of the term and status of their subscriptions continuously within their account settings. Regarding reminders, we believe that companies should retain sufficient flexibility to implement features that align with consumers' preferences and needs. For example, for long-term contracts, reminders tend to come either at a quarterly or annual basis. On the other hand, the experience of DOT Europe members has shown that consumers tend to find excessive notifications, in some cases monthly or more, irritating. Excessive obligations to send notifications could result in fatiguing consumers and them paying even less attention to subscription termination timelines, especially when receiving such notifications across multiple services at the same time. This reduced attention increases the risk of phishing, as lookalike emails are a well-established vector for scams. Similarly, the issue of consumers signing up for a paid service and forgetting about it raises the question of monitoring activity on the part of a company, which could only be achieved via extensive data collection. This problem can instead be dealt with by proper enforcement of rules concerning transparent information, timely reminders and easy cancellation.

Simplification measures

The European Commission is currently undertaking a comprehensive simplification effort, which should include the consumer acquis. This commitment should serve as a *fil rouge* guiding any activity on consumer protection rules, ensuring a proper assessment of their impact on legal complexity. To be effective and coherent, this approach must also be fully aligned with the EU's broader omnibus of digital regulations.

Impact of consumer information requirements and digitisation: Online service providers work diligently to ensure consumers are safe and well-informed while enjoying a seamless online experience. Various pieces of existing legislation (UCPD, CRD, Platform to Business Regulation, to name a few) regulate the information that must be provided to consumers, as well as the way this information has to be presented. The European Commission has already recognised the potential for information overload (e.g., the case of cookie notices), which is a positive step. Reducing information obligations for repetitive transactions with the same provider or those concluded via AI assistants also leads into the right direction. It is necessary to acknowledge and assess

the effect of this multitude of information on consumers and consider ways to simplify and reduce the information overload – especially in contexts which are inherently limited by time and space - and, avoiding overlapping or conflicting obligations or guidance from regulators.

We support providing consumer information in digital format. Providing information to consumers in digital form allows consumers to receive more relevant information, information that is up to date, available in more languages, as well as preventing environmental waste. Allowing for such an option in the shorter term and ahead of the unrolling of the digital product passport (DPP) will enable companies to build readiness in an achievable first step, and unlock the benefits of digitisation for consumers in a timely manner.

Horizontal issues

Protection of minors

Protecting minors online has been at the heart of EU policymaking in recent months and this is a debate DOT Europe welcomes. Our members take their responsibilities to younger users seriously and have already introduced a wide range of measures to promote safer, age-appropriate online experiences.

While Member States are rightfully pursuing initiatives to further enhance the protection of minors online, we are concerned that the introduction of national level legislation risks fragmenting the EU's harmonised approach to digital safety. This fragmented approach at Member State level must be avoided and likewise within the EU's own legislative framework, which addresses minor protection on relevant services from various angles: audiovisual, content moderation, systemic risks requirements, data protection and privacy, platform design, education, disinformation, media literacy, etc. each with different services in scope. Moreover, the Guidelines under Article 28 of the DSA have just been adopted by the Commission. These Guidelines provide recommendations and set expectations on how online platforms should comply with Article 28 obligations, including on topics such as commercial practices, account settings, online interface design and recommender systems, among others. While we recognise that more remains to be done to meaningfully address the risks that remain for children where they occur, we recommend that policy makers instead focus on the effective implementation of existing legal frameworks to their maximum extent before considering further proposals. This will increase the chances of thorough compliance by providers, and meaningful enforcement by regulatory bodies and enable a complete assessment of whether and where any gaps in legislation remain resulting in impactful changes where necessary.

Additionally, we would caution against any new requirements or references to age assurance (including age verification) in the DFA. Age assurance as a technology – while at times useful to gate children from proven high risks online – does not come without trade-offs. These can include risks to privacy (with varying degrees of privacy preservation), user experience, accessibility, and social inclusion. Any obligation to deploy age assurance must be targeted where there are demonstrable risks and thought through carefully to avoid any legal duplications. We recommend that to avoid fragmentation and duplication – particularly important in the era of regulatory simplification – policy makers instead prioritise the implementation of the DSA, including the Article 28 Guidelines. It would be important that the DFA not add additional uncertainty over the appropriate standards for age assurance.

Therefore, while we note the reference made to the protection of minors in the context of the DFA consultation, we do not see a need for an additional regulatory initiative on this topic at this time under the umbrella of the DFA. Efforts of the Commission, especially DG CNECT, should focus on clarifying the interplay between the different rules relevant to the protection of minors online and the implementation of DSA Article 28 in particular, in order to make the regulatory framework efficient, increase legal certainty for providers and protect minors online effectively.

Burden of proof and fairness by design

Changes to concepts such as 'average' and 'vulnerable' consumers, the reversal of the burden of proof, or the introduction of 'fairness by design' should be carefully considered in light of their potential impact on legal predictability and the EU's competitiveness.

Reversing the burden of proof, where traders are presumed to be non-compliant in response to a consumer claim until they can prove otherwise, would represent a significant shift from the current legal framework. This change would be overly burdensome and open to widespread abuse. It would force businesses to divert significant resources to legal and compliance matters, potentially having a chilling effect on growth and investment. The increased administrative effort and costs could then trickle down to consumers in several ways. For example, businesses might need to raise prices to offset these new expenses, which would reduce consumer purchasing power. Alternatively, they might cut back on investments in customer service, product innovation, or marketing, ultimately leading to a less satisfying customer experience. At a time when the EU is seeking ways to boost its competitiveness, it seems counterproductive to push businesses towards a more risk-averse and less innovation-driven mindset.

The existing consumer regulatory framework is already robust. Current laws, such as the Unfair Commercial Practices Directive and the Consumer Rights Directive, are designed to ensure traders provide clear, accurate, and timely information to consumers. These rules already mandate transparency and effective disclosure. For instance, traders are required to inform consumers about the main characteristics of a product, its price, delivery costs, and the existence of a right of withdrawal. Strengthening enforcement of these existing rules, rather than overhauling the system with a presumption of non-compliance, is a more effective way to address consumer protection concerns without imposing undue burdens on businesses.

Similarly, fairness is key to earning consumer trust and lies at the foundation of online services, affecting whether people choose a service and are willing to share data or pay for it.

A new, explicit Fairness by Design obligation is unnecessary and would add little to consumer protection, while increasing legal uncertainty for traders. Existing consumer law already embeds the principle from the outset, as companies need to take it into account when developing new products or services. Fairness by design is already reflected in pre- and post-contractual information obligations and prohibitions on dark patterns; and through general rules expressed in the negative, notably Article 5(1) of the UCPD: "Unfair commercial practices shall be prohibited."

A broad, positively worded catch-all duty to secure a fair online environment would be redundant and risk legal uncertainty. The same outcomes can be achieved by clarifying and enforcing existing rules through case law or guidance. Where specific problems are identified, they should be addressed with targeted, issue-specific legislation rather than an ambiguous Fairness by Design obligation.

Vulnerable consumers

The existing definitions of "vulnerable" and "average" consumers are well understood and tested in case law and hold significant value as a benchmark for policy making. In this regard, the CJEU has recently confirmed that the "average consumer" is a dynamic concept, which can continually adapt to protect consumers, including online. In its Compass Banca judgment of 14 November 2024, the Court underlined that the concept of the "average consumer" within the meaning of the UCPD does not exclude "the possibility that an individual's decision-making capacity may be impaired by constraints, such as cognitive biases". In doing so, the Court affirmed that the concept of the "reasonably well-informed and reasonably observant and circumspect" consumer is flexible enough to consider insights of behavioural research. There is thus no need to

adjust these definitions. Making a shift in the standard of consumer protection will come with significant repercussions to legal certainty and stability as well as the interpretation and enforcement of existing principles and rules.

In addition, the notion of vulnerable consumers is already covered in key pieces of legislation (GDPR, DSA, Accessibility Act), providing legal stability for companies. Broadening the scope, particularly with vague and subjective terms such as “emotional distress” or “negative mental state” risks diluting its impact and clarity. For example, identifying whether a consumer is “vulnerable” in that context would require the collection and processing of more personal data to identify at-risk consumers and could contradict the GDPR data minimisation principle. Instead, the focus should stay on specific at-risk groups, like minors, coupled with a risk-based approach that ensures protection, clarity and fairness.