Vereniging voor Reclamerecht

Statutair gevestigd te Amsterdam
Handelsregister Amsterdam 34235000

Input of the Study Committee on Digital Fairness of the Dutch Association for Advertising Law

for the Public Consultation on the Digital Fairness Act

Date: 23 October 2025

The study committee on Digital Fairness of the Dutch Association for Advertising Law (*Vereniging voor Reclamerecht*, "VvRr") is pleased to submit this contribution to the European Commission's public consultation on the proposed Digital Fairness Act ("DFA"). As a professional association representing experts in advertising and marketing law in the Netherlands, the VvRr is committed to promoting a balanced, effective, and future-proof legal framework for digital consumer protection.

Our input reflects the collective expertise of the members of the study committee on Digital Fairness and aims to support the European Commission's initiative to examine whether the European Union ("EU")'s existing consumer acquis provides effective and future-proof safeguards for fairness in the digital environment.

We respectfully submit the following observations and recommendations.

1. Dark Patterns

Single definition or scope delineation

"Dark patterns" is a term used in several (recent) EU directives/regulations (mostly in recitals), but its meaning seems to differ. While the idea is that the DFA builds upon existing frameworks such as the Unfair Commercial Practices Directive ("UCPD") and the Digital Services Act ("DSA"), a uniform legal definition of dark patterns or scope delineation is currently lacking. If the DFA intends to use the term 'dark patterns' in legal requirements, we recommend adopting a clear, harmonised definition aligned with existing EU acts that already address such practices. Such could be achieved by introducing an "omnibus"-like regulation which references the existing acts. In our view, it is especially important to clarify the relationship between dark patterns and unfair commercial practices. The DSA did not provide such clarification – on the contrary.

Leveraging existing documentation

While we support the development of further practical guidance under the DFA to aid enforcement and compliance, we emphasise that a substantial body of interpretive material already exists across instruments, including the GDPR, UCPD, and DSA, as well as in guidelines from bodies such as the European Data Protection Board ("EDPB"). Rather than duplicating these efforts, we recommend the adoption of open norms that are sufficiently specific to provide legal clarity while remaining adaptable

to evolving digital practices. This approach ensures coherence with existing frameworks and avoids regulatory fragmentation, while still offering meaningful protection against manipulative design practices. However, to avoid inconsistency in interpretation of terms across these regulations (like the term “dark pattern”) we would welcome the idea of a definition chapter in the DFA that clarifies and harmonises the terminology used across these (digital) regulations and directives.

2. Addictive Design and Gaming

Introduction

Throughout most Member States, an extensive legal and regulatory framework exists with respect to games of chance, colloquially referred to as “iGaming**”.** Providers of iGaming products are subject to strict requirements and are under national regulatory supervision. Prior to being permitted to offer iGaming products to consumers, providers need to apply for a licence and demonstrate, both as part of the licence application process as well as thereafter, that they comply with the applicable framework, are reliable and have the technical capacity and know-how to offer iGaming products in a safe and sustainable manner. Societal and scientific debates highlight the risks and negative effects of these practices in the eGaming sector, particularly concerning minors and their vulnerability to addiction.[1]

Whereas the traditional characteristic of iGaming products is the wagering of real money, the line between iGaming and ‘normal’ software games (also referred to as “eGaming”) has become blurry. Nowadays consumers can spend real money to enhance or improve their playing experience. Elements such as loot boxes and in-game purchases feature in most of the popular eGaming products, prompting and stimulating players to divert from the classical gaming experience to an experience that is similar to iGaming.

Clarify the difference between iGaming and eGaming

Despite the aforementioned extensive iGaming legal frameworks of EU Member States, eGaming is hardly regulated under EU law. There are no clear definitions for, and parameters to decide when a product is still and only an, eGaming product(s), preventing more hybrid categories of eGaming (which have iGaming elements) to be properly addressed. Furthermore, since iGaming is not a harmonised area of EU law, diverging practices throughout the EU exist regarding hybrid categories of eGaming (e.g. in some Member States lootboxes are allowed in eGaming, in others they are prohibited).

The DFA offers an opportunity to define and set clear boundaries between eGaming and iGaming products. That way, it is both clear which regulatory framework applies to these distinct market segments, as well how hybrid forms are to be addressed and classified.

Proposed measures to combat addiction to games

Once properly defined, the risks of eGaming products should be further set out and addressed. Similar to iGaming products, a risk classification could be made, classifying products from low to high risk. The risk factors and scores could be made based on a prior risk assessment, either done by an independent

[1] European Parliament July 202, Loot boxes in online games and their effect on consumers, in particular young consumers, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU(2020)652727_EN.pdf ; Wat is een Lootbox? Gokken voor kinderen

body (for a more objective assessment) or by the provider/developer of the eGaming product (with the risk of more subjective assessments).

Risk factors could be based on parameters currently used in iGaming risk assessments, such as event frequency, continuity of play, illusion of control and near win opportunities. The audiovisual design of the game should be considered as well.

Once a risk *classification* has been deployed, appropriate measures and safeguards could be set out which the provider of the eGaming product must install. Such measures could, for instance, include mandatory limits on playtime, limits on spending real money and the option to self-exclude from further playing.

On a national or EU-level, a self-exclusion register (similar to that of iGaming exclusion registers) could be put in place, where players suffering from or identifying addictive behaviours could self-exclude from further play for a certain period of time. Also, they could exclude their children. For instance, if there is a classification of (a) not addictive, (b) slightly addictive and (c) addictive, parents could register in a register comparable to the one built for secondary use of health data under the EHDS, that they themselves wish to have access to online products in category (a) and (b), while they want their children to have access to (a) only. Another possibility could be to make access illegal to a product or service in a category that one has self-excluded themselves from.

Although a system of regulatory supervision and licence requirements prior to being allowed to offer eGaming products, could hinder the freedom to provide services and cause a significant administrative load, such a system may be justified for the highest risk category of eGaming products, especially those with hybrid elements from the iGaming sector. A licence requirement could ensure providers of the highest risk category games have installed appropriate risk-mitigating factors and refrain from excessive or unnecessary stimulation of addictive game features, whereas regulatory supervision would provide a mechanism to hold such providers accountable.

Mitigate barriers for effective civil claims and redress

Consumers harmed by addiction, dark patterns, or other unfair practices in eGaming should have access to appropriate and proportionate remedies. The DFA could accommodate consumers in this regard, by providing clear definitions of what qualifies as compensable damages and what remedies are available to consumers.

By having harmonised definitions and remedies, the barrier for recovering damages, in or out of court, would be lower. National courts could provide for a special procedure for DFA claims whereby consumers would be able to recover damages and seek remedies in a transparent, efficient and cost-friendly manner (for instance by allowing for digital hearings and being able to recover all legal fees incurred by the consumer).

Currently, EU law solely states (as for instance in the GDPR):

> "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*."

It is left up to the Member states *how much* compensation is to be paid. For material damages this is not problematic: in every Member State this amounts to the actual damage caused which needs to be

compensated. For non-material damage however, this cannot be calculated in such a direct manner. In the Netherlands, courts generally award claims ranging between EUR 100 – 500 for non-material damages suffered as a result of a GDPR breach, which is low given the frequency and potential negative consequences that such a breach can have on individual persons.[2] This, combined with the fact that the losing party does not have to reimburse the winner's full legal costs, leads to the result that there is no effective redress, if there is solely non-material damage: the costs of going to court are far higher than the compensation awarded. Therefore, in all these instances where a breach of EU law is likely to be non-material damages, EU law should prescribe either a minimum compensation that needs to be paid, or it should prescribe that the full legal costs of the winner need to be paid (or both), because otherwise, there is no effective redress.

Prohibiting the processing of personal data for designing addictive products or services?

The European Health Data Space Regulation (EHDS) contains (article 54) a list of prohibited secondary use of health data. Among others: prohibited is the use of health data to develop products or services which are designed or modified in such a way that they create addiction. This leads to the following questions: (i) it remains unclear what the material scope of chapter IV of the EHDSR is and therefore it remains unclear what the material scope is of this list of prohibited secondary use (meaning: does the prohibition always apply to data users as this is maximum harmonisation, or does it apply solely when a data user voluntarily applies for a permit. In other words, is it allowed to bypass the Health Data Access Body, work under member state law and accomplish in this way that one does not have to adhere to the list of prohibited use?) (ii) Is it possible/ useful to harmonise this prohibition on using data to create addiction from health data to *other* types of personal data? (iii) Does it make sense to simply write in the DFA that an article will be added to the GDPR stating that it is forbidden to process personal data with the intention of designing addictive products or services?

3. Influencer Marketing and Social Media

Harmonised EU disclosure rules for influencer advertising, supported by platform obligations to enable disclosure-by-design

Our recommendation is that the DFA should establish one EU-wide baseline for disclosure of influencer marketing:

- **Require standard terminology** that is uniform across the EU, with translation into national languages where relevant and avoiding open norms as much as possible.
- **Require clearly visible disclosure** to the average consumer. We recommend the DFA provides clear instructions and examples on how this visibility should be achieved across different formats (e.g. posts, stories, short videos, livestreams).[3]

[2] In contrast, a recent district court ruling in Germany awarded EUR 5.000 for compensation of immaterial damages for a GDPR breach, showcasing the divergence in approach between Member State courts. LandGericht Leipzig 4 July 2025, 05 O 2351/23, https://rewis.io/urteile/urteil/hiy-04-07-2025-05-o-235123/.

[3] For a good example of this we refer to:

- https://www.reclamecode.nl/nederlandse-reclame-code/bijzondere-reclamecodes/#reclamecode-social-media---influencer-marketing--rsm-
- https://www.acm.nl/nl/publicaties/leidraad-bescherming-online-consument

In these codes, the supervisor or the sector organization provides direction and clarity to market parties in the context of self-regulation. The codes contain recommendations, practical instructions or additional explanations.

- **Platform duty:** social media and content-sharing platforms must provide disclosure-by-design tools (e.g. compulsory "#ad" toggles, permanent badges), so that influencers and advertisers have straightforward and uniform ways to comply.

We believe uniformity and clarity across Member States are vital. Well executed it: (i) ensures consumers can immediately recognise commercial content and reduces exposure to misleading commercial practices, (ii) provides legal certainty for companies and influencers, ensuring they know exactly what is expected to comply by removing ambiguity and room for diverging interpretations and (iii) avoids fragmentation across Member States.

Self-regulation as a compliance accelerator

National and EU authorities face limited enforcement capacity. At the same time, well-established self-regulatory bodies—such as the *Reclame Code Commissie* (RCC) in the Netherlands—already provide accessible, low-threshold complaint mechanisms.[4] Yet businesses and influencers that actively comply with these frameworks receive little recognition at the regulatory level, which reduces incentives for proactive compliance.

The DFA could address this gap by introducing reduced regulatory burdens and other incentives for companies and influencers that:

- demonstrate adherence to recognised national self-regulation codes,[5]
- complete certification or educational programmes (raising awareness of the rules they must follow),[6] and
- maintain strong compliance records with self-regulatory bodies.

Such a system would reward proactive compliance, promote a culture of responsibility, and allow authorities to concentrate resources on systemic abuses and serious violations. At the same time, consumers benefit from quick, low-cost, and easily accessible complaint procedures.

One example of such an incentive could, for example, be a trusted EU "compliance label" for influencers and brands who participate in approved self-regulation and education schemes.

Sector initiatives

In several Member States, the advertising and influencer marketing sectors have already developed initiatives to improve compliance and transparency of influencers on social media. In the Netherlands, the industry has launched a certification for influencers to ensure they are aware of both statutory and self-regulatory advertising rules. Similar initiatives exist in other EU countries, such as France, Belgium, Spain, and Romania. They are all part of AdEthics, a European umbrella initiative for national influencer education. Early results are promising in the Netherlands: compliance with advertising rules increased from 25% to 60% after certification, showing measurable impact while underlining that recognisability remains a key area for improvement. Therefore, we advise focusing on recognisable disclosures.

4. Personalisation and Profiling Practices

Personalisation and profiling practices refer to the adjustment of online content—such as prices, advertisements, product rankings, or user interfaces—based on a consumer's characteristics or behaviour. This can include location, browsing history, purchase patterns, or demographic data, with

[4] https://www.reclamecode.nl/klacht-indienen/klachtenformulier/
[5] See footnote 1
[6] An example from the Netherlands: https://influencerregels.com/certified-by/

the aim of tailoring the experience to individual preferences or needs. Therefore, one of the main questions regarding these practices is: what does the European Commission wish to codify within a DFA?

Right now, personalisation and profiling current provisions concern the following:

1. **Transparency**: Businesses must clearly inform users when personalisation is used—especially for prices, ads, or product rankings.
2. **Fairness**: Exploiting consumer vulnerabilities (e.g. financial distress) through personalisation is prohibited.
3. **GDPR Compliance**: Profiling is considered automated processing of personal data. It requires a lawful basis (e.g. consent or legitimate interest) and must include safeguards like human intervention and explanation rights.
4. **DSA**: Platforms must explain how personalised recommendations work and offer users a non-profiled alternative. Targeted ads based on sensitive data or aimed at minors are banned.
5. **Enforcement by The Netherlands Authority for Consumers and Markets ("ACM")**: The Dutch regulator enforces transparency in personalised pricing and prohibits misleading or manipulative practices.

What's Missing in EU Law to Ensure Transparency in Personalisation and Profiling? Despite existing provisions under the GDPR, DSA, and consumer protection directives, several gaps remain:

1. **Fragmented obligations**: Transparency requirements are spread across multiple laws (GDPR, DSA, UCPD), making it hard for businesses to understand and comply consistently.
2. **Lack of clarity on profiling impacts**: Current laws do not require businesses to explain *how* profiling affects prices, recommendations, or user experience in a meaningful, user-friendly way.
3. **Limited enforcement tools**: Supervisory authorities lack harmonised mechanisms to monitor and enforce transparency obligations across platforms and sectors.
4. **Insufficient protection against exploitative personalisation**: There are no clear rules preventing companies from using personalisation to exploit consumer vulnerabilities (e.g. targeting financially distressed users with risky offers).
5. **No standard for meaningful explanation**: GDPR requires transparency, but does not define what constitutes a "clear and understandable" explanation of automated decision-making or profiling.
6. **No default opt-out for profiling**: Consumers often have no easy way to opt out of personalisation, and platforms are not required to offer non-profiled alternatives unless they are Very Large Online Platforms (VLOPs) under the DSA.

Our recommendations with respect to Personalisation and profiling practices are:

Introduce a unified transparency standard

Require businesses to provide clear, consistent, and user-friendly explanations of how personal data influences prices, recommendations, and content—across all digital services.

Mandate default opt-out options for profiling

Ensure all consumers - not just users of Very Large Online Platforms - can easily choose a non-profiled experience, with clear controls and no penalty in functionality.

Ban exploitative personalisation practices

Explicitly prohibit personalisation that targets vulnerable consumers (e.g. minors, financially distressed individuals) with manipulative offers or pricing.

Define 'meaningful explanation' in profiling

Clarify what constitutes a "clear and understandable" explanation under GDPR and DSA, especially for automated decision-making and profiling.

Strengthen enforcement mechanisms

Equip regulators with harmonised tools (e.g. automated market sweeps, joint enforcement powers) to monitor and enforce compliance across Member States.

Simplify the legal framework

Consolidate fragmented obligations from GDPR, DSA, UCPD, and other directives into a coherent and accessible set of provisions for businesses and consumers.

Enhance protection for minors

Require age-appropriate design, stricter age verification, and prohibit profiling-based advertising for minors across all platforms.

Ensure algorithmic accountability

Require platforms to disclose the logic and criteria behind algorithmic recommendations and pricing, and allow users to challenge or review automated decisions.

Consider sector-specific provisions

Some goods and services might evoke more vulnerabilities than others, for example because of high dependence on a certain product or little alternatives. Inspiration can be found in Article 13 of the Consumer Credit Directive (Directive 2023/2225, CCD). This Directive contains a pre-contractual information requirement similar to that of Article 6 Directive 2011/83/EU and limits the scope of data processing by creditors and credit intermediaries: they have to limit their analyses to assessing the creditworthiness of a consumer and in doing so, they cannot process special categories of data, such as the sensitive data ex Article 9 (1) GDPR (see Recitals 55 and 57 CCD).

Clarity regarding the relationship between the DFA and Directive 2019/770 (Digital Content Directive)

Little attention is given to the interplay between the DFA and Directive 2019/770. For example, it is quite conceivable that consumers are not informed about prices being personalised on the basis of automated decision-making (exarticle 6 Directive 2011/83/EU) in the context of transactions involving

digital content or services. This could lead to a conflict with the conformity requirement in the Directive 2019/770, implemented as Article 7:50ae in the Dutch Civil Code.

5. Digital Contracts and Subscription Models

There are valid concerns around online services that make cancellation unnecessarily difficult or continue renewals without sufficient transparency. However, new overly rigid requirements — such as one-click cancellation or very frequent reminder obligations — could risk undermining legitimate long-term subscription models that deliver predictable value to consumers. Therefore, we recommend that the DFA should ensure cancellation and renewal provisions are clear, fair, and proportionate.

Cancellation procedures should be easy to understand and accessible for consumers, but should also allow for reasonable safeguards against fraud, accidental cancellations, or misuse.

Consumers should receive transparent information about their subscriptions, but excessive reminder obligations could create unnecessary disruption and confusion. There should be a good balance between ensuring informed choice while preserving stability in long-term subscriptions.

We recommend that the DFA explicitly distinguishes between abusive subscription traps and legitimate long-term subscription models, ensuring that new provisions only target truly harmful practices.

Industry self-regulatory initiatives, such as clear model terms for digital contracts and transparent subscription management tools, can complement statutory requirements and promote consumer trust. The DFA should encourage the development and adoption of best practices for digital contracts and subscriptions, foster public-private cooperation, and support consumer education campaigns to raise awareness of rights and remedies in the digital environment. This approach will enable rapid adaptation to technological change and evolving consumer expectations, while minimizing regulatory burdens.

6. Interplay with other EU Legislation

One of the most important issues is the inter-relationship between the envisaged DFA and the extensive body of EU legislation that already governs business-to-consumer communications, digital service design and the processing of data. In view of the rapidly expanding rulebook, our primary concern is to preserve legal certainty and coherence while preventing overlapping – and potentially conflicting – obligations for advertisers, media owners and digital intermediaries operating across the Single Market.

Between 2018 and 2024 the EU adopted a sequence of landmark instruments – the GDPR, the e-Privacy regime (Directive 2002/58 as interpreted by the Court of Justice), the Modernisation Directive amending the UCPD and CRD, the DSA, DMA, AI Act and Data Act – each containing directly enforceable provisions designed to curb the very practices highlighted in the Digital Fairness Fitness Check: manipulative interface design, intrusive profiling, lack of advertising transparency, subscription traps and addictive mechanics. These texts are complemented by sector-specific measures such as the AVMSD for audiovisual commercial communications and the forthcoming European Health Data Space Regulation (EHDSR) for health-related data use.

The aggregate result is a *principle-based, technology-neutral and already future-proof* architecture. Any new act must therefore be positioned as lex generalis of last resort; otherwise there is a serious risk of duplication (e.g. a second set of “dark-pattern” prohibitions mirroring DSA Article 25) and of regulatory fatigue among the national authorities expected to enforce the legal framework.

Please find below some key interfaces that require particular attention:

Existing Instrument	**Coverage most relevant to advertising & consumer interactions**	**Potential conflict / duplication if the DFA proceeds without alignment**
Digital Services Act (Reg. 2022/2065)	Art. 25 dark patterns; Arts 26–28 advertising transparency, sensitive data targeting and bans on profiling minors; Art. 34 systemic risk mitigation for interface-driven harms.	A parallel DFA prohibition might diverge in definitions ("manipulative design" v. "dark pattern") or in enforcement allocation, undermining the DSA's country-of-origin logic and the role of Digital Services Coordinators.
Digital Markets Act (Reg. 2022/1925)	Art. 13 anti-circumvention and design obligations on gatekeepers; consent requirement before cross-use of personal data.	Any DFA provision on "fairness by design" must not impose alternative consent standards or interface duties that fracture the DMA gatekeeper regime.
AI Act (Reg. 2024/1689)	Prohibits subliminal/manipulative AI systems and establishes risk-based duties; Art. 14 human oversight.	A DFA extension of "algorithmic fairness" could unintentionally recast advertising or recommendation engines as a new risk class, contradicting the AI Act's tiered taxonomy.
Data Act (Reg. 2023/2854)	Recital 38 prevents dark patterns in consent flows for data-sharing.	Additional DFA consent-form rules would load a third, diverging set of interface standards on data holders and recipients.
GDPR & e-Privacy	Lawful basis constraints, special-category data ban, transparency arts. 12-14, rights to object (Art. 21) and automated decision safeguards (Art. 22).	A DFA prohibition on "profiling vulnerable consumers" must dovetail with GDPR sensitive-data concepts to avoid parallel interpretations and enforcement fora.
UCPD (Dir. 2005/29)	Annex I already outlaws aggressive practices, including hidden advertising by influencers, false urgency claims, and subscription obstacles; the 2021 Guidance expands to dark patterns.	Re-legislating the UCPD blacklist at DFA level would fragment thirty years of harmonised case law and disrupt the "maximum harmonisation" principle.
CRD (Dir. 2011/83)	Art. 11a single-click withdrawal; Art. 6 explicit payment acknowledgment; tailored provisions on free trials.	Any DFA attempt to mandate additional unsubscription buttons or renewal notices must be evaluated against ongoing transposition of Modernisation Directive amendments.

AVMSD (Dir. 2018/1808)	Arts 9 & 28b on commercial communications, influencer declarations, and protection of minors.	A DFA influencer regime that differs in scope or sanctions could create diverging standards between video-sharing services and other platforms.
EHDSR (Reg. 2025/327)	Secondary use of electronic health data and associated advertising constraints.	A DFA clause on "health-related vulnerability profiling" must be consistent with EHDSR re-use permissions to avoid contradictory compliance expectations.

The various legal instruments above allocate monitoring and sanctioning powers to distinct, and sometimes newly created, enforcement authorities. Overlaying a further horizontal act could scatter enforcement competences. See also under the heading Enforcement below.

To ensure consistency and prevent overlap, the DFA should expressly state that it is without prejudice to the DSA, DMA, AI Act, Data Act, GDPR/e-Privacy, UCPD, CRD, AVMSD and EHDSR. Second, rather than imposing additional substantive prohibitions, the DFA should clarify how the existing rules interlock, specifically in the advertising and platform context.

Against this background, it could even be considered whether adding more additional rules to the current legislative framework is a feasible approach, or whether it is better to reflect on the current acquis, and give priority to applying and aligning the existing regulatory arsenal.

7. Enforcement

Enforcement, more than legislative deficits, are the primary source of consumer detriment

The Commission's own Fitness Check recognises that most of the harmful practices at issue—deceptive interface design, disguised advertising by influencers, drip pricing, subscription traps, exploitative personalisation—are already captured by existing horizontal instruments such as the Unfair Commercial Practices Directive and the Digital Services Act. The persisting €7.9 billion annual detriment therefore points to weaknesses in detection, investigation and sanctioning rather than legislative lacunae. Before introducing new obligations, the Union should prioritise a clear enforcement strategy that (i) provides national authorities with adequate financial, technological and human resources, (ii) ensures consistent interpretation through binding guidance, and (iii) enables coordinated sweeps and joint investigations for large-scale cross-border practices.

Avoid parallel enforcement hierarchies and ensure one "single point of supervision" per practice

Digital traders already face multiple regulators under sector-specific regimes (for example: media regulators under the AVMSD, data-protection authorities under the GDPR, Digital Services Coordinators under the DSA, competition authorities under the DMA and national consumer authorities under the CPC Regulation). Overlapping mandates generate conflicting orders, forum shopping and compliance dead-weight costs—particularly for SMEs that drive innovation in advertising technology. The DFA should, therefore, either (a) designate a lead authority – potentially with cross border authority for the entire EU – for each category of practice (dark patterns, influencer marketing, addictive design, personalised pricing) and mandate structured cooperation between that lead and the competent sectoral authorities, or (b) integrate enforcement into the existing CPC framework, thereby

preserving the benefits of Regulation (EC) 2006/2004 while extending its investigative toolkit to cover algorithmic systems and platform design.

Promote public–private partnerships and self-regulatory codes

Advertising self-regulatory systems, such as the Dutch Advertising Code and the pan-European ICC Advertising and Marketing Communications Code, have long provided agile enforcement, fast dispute resolution and credible sanctions (public decisions, mandatory withdrawal of advertising, fines). The DFA should endorse and leverage these mechanisms where they demonstrably uphold Union standards, reducing the enforcement burden on public bodies while delivering speedy redress. Co-regulatory memoranda of understanding could require platforms to enforce self-regulatory decisions and to remove or demote content that violates both the self-regulatory code and Union consumer law.

Ensure that enforcement measures remain technology-neutral and future-proof

The digital advertising ecosystem evolves rapidly; prescriptive design mandates (e.g. fixed font size or colour for cancellation buttons) risk obsolescence and may inadvertently restrict innovative, consumer-friendly interfaces. Enforcement should therefore be grounded in outcome-based criteria rather than rigid form-based tests. Authorities should be encouraged to publish illustrative, non-exhaustive examples and to update them periodically through stakeholder consultation.

8. Non-regulated topics (such as the Average Consumer standard)

We recommend that the DFA includes sufficiently concrete, practical guidance on how to apply the "average consumer" standard in digital contexts. Clear guidance on this topic could increase legal certainty for responsible operators, while ensuring fair and – due to its harmonization – more consistent protection for consumers. It could also prevent less compliant actors from exploiting national differences in interpretation, by ensuring a level playing field.

At the same time, it is important to ensure that responsible operators are enabled to continue to use legitimate and effective digital marketing tools without disproportionate restrictions. Regulators should be enabled to concentrate resources on practices with genuine and serious harmful effects.

The findings of the present Fitness Check suggest that there is a disparity between the reality of consumer behaviour in the digital environment and the normative expectations in law regarding the 'average consumer'.

The position that the EC took in the UCPD Guidance, that the vulnerability characteristics highlighted in 5(3) UCPD are non-exhaustive and that the concept can be interpreted in a dynamic and situational manner, seems like a promising foundation. However, the concept of the average consumer is even more faceted and granular; it requires empirical research to further assess the circumstances that can influence the way one moves through the digital environment.

Specific examples of vulnerability in *inter alia* the GDPR, DSA and AI Act can exist next to a more broad, open-ended interpretation of vulnerability as a concept without there being unacceptable contrast.

Keep in mind that it is not only the concepts of 'average' and/or 'vulnerability' that require further exploration, but also the concept of 'consumer' itself. There are at least three, non-mutually exclusive categories of consumers: (1) the digital consumer, who is constantly being nudged by largely invisible online marketing strategies, (2) the prosumer, who also interacts with platforms as a business user (e.g., seller on online platforms such as Vinted; see also P2B Directive) and (3) the (aspiring) green consumer, who should (or wishes to) play a role in sustainability

Clarifications, amendments or guidance regarding the average consumer would mainly impact consumer law rather than contract law. However, it is thinkable that changes in assumptions underlying contract law could also require changes in contract law.

9. Conclusion

From the perspective of the study committee on Digital Fairness of the VvRr, for the DFA to achieve the objectives as communicated by the Commission, the DFA must deliver clear and coherent definitions, align seamlessly with the existing EU legal framework, and avoid creating overlapping or conflicting obligations for businesses and regulators. Effective enforcement and accessible redress mechanisms— especially for non-material damages — are essential to ensure real consumer protection. In our view, the DFA should address specific risks such as addictive design, exploitative personalisation, and the safeguarding of minors, while also supporting innovation and legal certainty for responsible operators.

On behalf of the study committee on Digital Fairness of the Dutch Association for Advertising Law,

R.W. de Vrey and M. Poulus (co-chairs), J. van Balen, S. Baneke, N. Boomsma, K. Heidary, J. Jacobi, R. van der Leij, R. Pull Gunne, J. Reus, M. Smulders, A. Vlieger, A. Hosli and J. Julicher

The contents of this document reflect the personal views of the members of the study committee and do not necessarily represent the views of the VvRr