cerre

TOWARDS AN EU CONSUMER LAW FIT FOR THE DIGITAL AGE

REPORT

February 2026

Christoph Busch
Amelia Fletcher
Michèle Ledger

As provided for in CERRE's bylaws and procedural rules from its “Transparency & Independence Policy”, all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Apple, CnaM, Snapchat, Temu, Tencent, and TikTok. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu –www.cerre.eu

Executive Summary

The forthcoming proposal for a Digital Fairness Act (DFA) is a key priority of the European Commission's 2030 Consumer Agenda. Expectations are high for the proposal, which is expected for Q4/2026. The DFA needs to balance the concerns of competitiveness, ensuring a high level of consumer protection and creating a genuine EU Digital Single Market.

Against this background, this report explores key topics that are currently at the centre of the debate about the future of EU consumer law. We focus on five aspects: (1) horizontal issues relating to overarching concepts and principles of consumer law, (2) issues with digital contracts and subscriptions, (3) protection of minors in digital environments, (4) addictive design features, and (5) personalisation practices. For these topic areas, the report provides the following actionable recommendations:

Recommendations for horizontal issues

1.1 The DFA should focus on filling regulatory gaps and simplifying the existing framework of consumer protection. It is particularly important to ensure a frictionless interplay between the DFA and sector-specific rules, in particular the DSA. Where existing rules are extended to a wider set of players it should be clear that meeting the sector-specific regulation would constitute compliance with the DFA.

1.2 The DFA should be based on three general principles for smart digital regulation: (i) risk-based regulation, (ii) design-based regulation, and (iii) ecosystem regulation.

1.3 Risk-based regulation: The DFA should address clearly identified problems only where they arise and ensure that traders unaffected by those problems are not overburdened. This means that the DFA should differentiate between business models according to their specific risk profile.

1.4 Design-based regulation: To ensure effective consumer protection, the exercise of consumer rights must be facilitated by designing the user interface in such a way that consumers can easily exercise their rights.

1.5 Ecosystem regulation: B2C contracts are typically embedded in a broader ecosystem with a variety of players. Policy interventions should ensure that all players contribute to ensuring compliance and effective enforcement of consumer law.

1.6 The concept of 'fairness by design' should be introduced as an interpretative principle linked to the concept of professional diligence (Art. 2(h) UCPD) rather than as a new stand-alone obligation.

1.7 It does not seem necessary to fundamentally revise the current benchmark of the 'average consumer'. However, as a matter of clarification, it could be helpful to codify the more recent CJEU case law, for example, in the recitals of the DFA. In doing so, the systemic and situational aspects of 'digital vulnerability' should be taken into account when applying the 'average consumer' concept.

Recommendations for digital contracts and subscriptions

2.1 Regulation of subscription models in the DFA should be risk-based and differentiate between business models according to their specific risk profile. More specifically, policy interventions could be differentiated according to different categories of products (e.g. physical products, services, digital content) and the duration of the contract renewal.

2.2 The DFA should follow a design-based approach. This means that the exercise of consumer rights should be facilitated by consumer-friendly user interface design, for example through the introduction of an easy cancellation facility. The design requirements should be accompanied by guidance and illustrations of best practice.

2.3 Regulation of subscriptions in the DFA should be based on an ecosystem approach and give thought to the roles and responsibilities of all actors in the 'subscription stack' including app stores, online marketplaces as well as providers of payment services and subscription management tools.

2.4 If the DFA introduces a right of access to a human interlocutor in consumer services, such a regulation should not be too burdensome for start-ups and SMEs. One option could be to introduce such a right only for contracts above a certain financial volume.

Recommendations for minors

3.1 There is a lack of horizontal rules at the EU level to protect minors online: some sector specific rules exist but not all players are covered. Sector specific rules are not consistent and there are overlaps. The internal market is also fragmented. Therefore, the DFA could provide some level of protection for minors in their relationship with all online traders.

3.2 The DFA could build on the current approach of the Unfair Commercial Practices Directive (**UCPD**), which considers that minors can be vulnerable consumers, and extend this to consumer protection law more generally.

3.3 The DFA will need to acknowledge and address the overlap with sector specific rules, especially the way these rules are enforced (by regulators for sector specific rules).

3.4 The DFA should not seek to address the fundamental societal question of a potential social media ban for minors.

3.5 To address the unlevel playing field, the DFA should prohibit online traders from presenting advertisements based on profiling (as defined in the GDPR) by using the personal data of minors (to the extent that they are aware, with reasonable certainty, that they are minors).

3.6 To the extent that the DFA introduces specific rules to protect minors, age assurance needs to be addressed. We recommend that the DFA refers back to what is specified in the Article 28 DSA guidelines when it comes to age verification and/or age assurance.

Recommendations for addictive design

4.1 Any regulation needs to be carefully designed, if the positive aspects of potentially addictive design features are not to be lost for those that engage responsibly online. In addition, overly intrusive regulation could risk pushing vulnerable users towards deliberate circumvention or even into less safe unregulated spaces.

4.2 Legislation for addictive design should ensure that it is sufficiently risk-based to enable different design features, users and contexts to be treated differently, including over time.

4.3 Legislation for addictive design should seek to increase the availability and use of enhanced controls. Consideration should also be given to setting controls as 'safe by default', especially for minors.

4.4 Legislation for addictive design should enable (and possibly require) enhanced activity, spending and notifications controls to be set at system-level, which service providers can then rely on for their compliance. Controls relating to specific addictive design features should be set at individual service level.

4.5 The Commission should consider using the DFA to strengthen requirements in relation to these system-level activity, spending and notifications controls.

4.6 The Commission should use the DFA to require the risk-based adoption of enhanced controls and defaults for specific addictive design features (and in extreme cases prohibitions for certain users).

4.7 Rather than seeking to address specific addictive design features by refining the UCPD, it would be more coherent to introduce a new targeted rule within the DFA.

4.8 The Commission should consider introducing a targeted rule within the DFA for design features that are persuasive, aimed predominantly at engagement, and create a risk of harm in the form of extensive use or overuse of the platform or problematic or compulsive behavioural habits. Firms employing such design features should provide controls, and implement default settings, that address the risk of harm; ensure effectiveness though making these controls are easy to access, understand and use, and designing in sufficient friction associated with diverging from the default; and ensure that the risk is specifically addressed for vulnerable users, including minors.

Recommendations for personalisation practices

5.1 Following the principle of risk-based regulation, the DFA should focus on addressing clearly identified harms of personalisation practices and ensure that consumers do not lose the benefits of personalisation. With a view for the principle of proportionality, different use cases may require different depth of regulation (opt-out, opt-in, ban).

5.2 The Commission should consider introducing a rule that requires businesses to provide a simple opt-out option for personalised advertising or offers. A simple but effective solution could be a standardised 'privacy button' modelled on the recently introduced withdrawal button (Art. 11a CRD).

5.3 To ensure a level playing field, the DFA should extend the prohibition of advertising based on special categories of personal data as defined in the GDPR (see Art. 26(3) DSA) and targeted advertising addressed to minors (see Art. 28(2) DSA).

5.4 The DFA should prohibit personalised advertising that exploits the specific vulnerabilities of a consumer, including temporary and situational vulnerabilities (e.g. emotional targeting).

Table of Contents

EXECUTIVE SUMMARY 1

Recommendations for horizontal issues 1
Recommendations for digital contracts and subscriptions 2
Recommendations for minors 2
Recommendations for addictive design 3
Recommendations for personalisation practices 3

INTRODUCTION 7

1. HORIZONTAL ISSUES 10

1.1 Three General Principles for Smart Digital Regulation 10
1.1.1 Risk-Based Regulation 10
1.1.2 Design-Based Regulation 11
1.1.3 Ecosystem Regulation 11
1.2 Fairness by design 12
1.3 Concepts of Average/Vulnerable Consumer 13
1.3.1 Average consumer 13
1.3.2 Vulnerable consumer 14

2. DIGITAL CONTRACTS 15

2.1 Introduction 15
2.2 The Rationale for Regulation in this Area 15
2.2.1 Concerns regarding digital contracts 15
2.2.2 Is there a Regulatory Gap? 16
2.3 The Commission's Possible Policy Measures 17
2.3.1 General Principles for Policy Intervention 17
2.3.2 The Commission's Possible Policy Measures 19

3. PROTECTION OF MINORS 24

3.1 Horizontal Rules on the Protection of Minors: GDPR and the Consumer Protection Acquis 24
3.1.1 The Consumer Protection Acquis and the Concept of Vulnerable Consumer 25
3.2 Sector Specific Rules on the Protection of Minors: Audiovisual Media Services Directive, the DSA and the AI Act 25
3.3 Unlevel Playing Field and Internal Market Fragmentation 28
3.4 How Could the DFA Address the Lack of EU Rules to Protect Minors Online? 29
3.5 The DFA Needs to Take into Account the Interplay of Rules 31

4. ADDICTIVE DESIGN 33

4.1 THE RATIONALE FOR REGULATION IN THIS AREA 33
4.1.1 CONCERNS ABOUT ADDICTIVE BEHAVIOUR 33
4.1.2 CONCERNS ABOUT ADDICTIVE DESIGN 34
4.1.3 BENEFITS OF 'ADDICTIVE DESIGN' FEATURES 35
4.1.4 IS THERE A REGULATORY GAP? 36
4.2 DESIGNING PROPORTIONATE, EFFECTIVE REGULATION 40
4.2.1 GENERAL PRINCIPLES FOR POLICY INTERVENTION 40
4.2.2 OPTIONS FOR POLICY INTERVENTION 45
4.2.3 THE COMMISSION'S POSSIBLE POLICY MEASURES 49

5. PERSONALISATION PRACTICES 52

5.1 INTRODUCTION 52
5.2 THE RATIONALE FOR REGULATION IN THIS AREA 52
5.2.1 CONCERNS REGARDING PERSONALISATION PRACTICES 52
5.2.2 IS THERE A REGULATORY GAP? 53
5.3 THE COMMISSION'S POSSIBLE POLICY MEASURES 54
5.3.1 GENERAL PRINCIPLES FOR POLICY INTERVENTION 54
5.3.2 THE COMMISSION'S POSSIBLE POLICY MEASURES 55

ABOUT CERRE 59

ABOUT THE AUTHORS 60

Introduction

In October 2024, the European Commission presented its long-awaited final report on the Digital Fairness Fitness Check,[1] which evaluated three EU consumer law Directives[2] and analysed whether the existing EU consumer law framework is still relevant, effective and efficient in the current digital environment. The Commission report concluded that EU consumer law, as it stands today, provides the necessary minimum of regulatory certainty and consumer trust, but the existing regulatory framework can be considered only partially effective in the digital environment.[3] In particular, the report identifies a variety of concerns, such as transparency in advertising and pre-contractual information; problems associated with emerging technologies and practices for which there are no specific provisions in the current EU consumer law legislation; regulatory fragmentation which undermines the Digital Single Market; increasing regulatory complexity arising from wider digital-specific regulation which is relevant for consumer markets, such as the DSA, the DMA or the AI Act; and also more general issues relating to insufficient compliance, ineffective enforcement and legal certainty.

In addition to these general concerns, the Commission report highlights several "problematic practices".[4] The areas of concern identified by the Commission range from market practices that it considers insufficiently well addressed by existing legislation (e.g., harmful online choice architecture (dark patterns) and difficulties in managing digital contracts) to emerging technologies and market practices for which there are limited or no specific provisions in existing EU consumer law (e.g., addictive design features, unfair personalisation practices that exploit consumers' vulnerabilities and harmful practices by influencers).[5] According to the Commission, the estimated financial detriment suffered by consumers as a result of the identified problems is at least EUR 7.9 billion per year.[6]

In December 2024, the Commission announced that it intends to propose a Digital Fairness Act (DFA) to address the issues identified in the Digital Fairness Fitness Check. In her mission letter to the Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, Michael McGrath, Commission President Ursula von der Leyen, called for the development of "a Digital Fairness Act to tackle unethical techniques and commercial practices related to dark patterns, marketing by social media influencers, the addictive design of digital products and online profiling, especially when consumer vulnerabilities are exploited for commercial purposes".[7]

From July to October 2025, the Commission conducted a public consultation on the forthcoming DFA.[8] The DFA also features prominently in the 2030 Consumer Agenda which was published in November

[1] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*, SWD(2024) 230 final.
[2] The Digital Fairness Fitness Check focused on the Unfair Commercial Practices Directive 2005/29/EC (UCPD), the Consumer Rights Directive 2011/83/EU (CRD), and the Unfair Contract Terms Directive 93/93/EEC (UCTD).
[3] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*, SWD(2024) 230 final, p. 36.
[4] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*, SWD(2024) 230 final, p. 146-203.
[5] The non-binding UCPD Guidance 2021 does address some of these issues, e.g. personalisation, dark patterns and influencer marketing, see European Commission, Guidance on the interpreation and application of Directive 2005/29/EC, OJ C 526, 29.12.2021, pp. 1-129.
[6] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*, SWD(2024) 230 final, p. 27.
[7] President of the European Commission, Mission Letter to Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection Michael McGrath, 1 December 2024, p. 7.
[8] The summary of the consultation was published in December 2025: European Commission, Public consultation on the Digital Fairness Act, Factual Summary Report, December 2025, Ares(2025)11434262 - 19/12/2025.

2025.[9] At the time of writing, the Commission is preparing the Impact Assessment for the DFA. According to the Commission work programme, a legislative proposal is expected for Q4/2026.[10]

CERRE has been continuously contributing to the debate on the future of EU consumer law. In May 2024, we published a CERRE Report on Harmful Online Choice Architecture which was intended to feed into the Digital Fairness Fitness Check.[11] Following the publication of the final report on the Fitness Check, in December 2024 we published a CERRE Issue Paper that addressed some of the overarching questions surrounding a future DFA.[12] Further input for the policy debate was provided through a series of CERRE Issue Papers focusing on the protection of minors.[13]

In the meantime, the policy debate has progressed further and the possible contours of a DFA are beginning to emerge. Before delving into the details, three general remarks regarding the broader political context are in order:

First, it is becoming increasingly clear that the DFA will have a particular focus on the protection of minors. While this undoubtedly is an important policy objective, it poses a challenge for the architecture of EU consumer law. Introducing specific consumer rights for minors will increase the complexity of the regulatory landscape. Moreover, adults may also be vulnerable to harms such as addictive design and unfair personalisation.

Second, it is worth noting that although the forthcoming DFA is framed as a consumer law instrument, it is likely to extend beyond the scope of the legislative acts examined in the Digital Fairness Fitness Check. In contrast to the UCPD, CRD, and UCTD, the current regulatory debate surrounding the DFA is not confined to the economic dimensions of consumer policy. Rather, it also encompasses non-economic harms and wider societal concerns, most notably the protection of minors. In this sense, the policy debate on the DFA is situated within a wider discussion on the evolving contours and objectives of consumer law.[14]

Finally, the policy debate on the DFA unfolds against a backdrop of increasing political emphasis on competitiveness, regulatory simplification, and the need to strengthen the single market. As a result, the threshold for introducing additional regulatory requirements is set relatively high. At the same time, consumer protection should be recognised not only as an objective in its own right, but also as a potential driver of competitiveness. In particular, a predictable and trustworthy consumer protection framework can facilitate market entry for small firms and start-ups by ensuring a level playing field for all market participants, irrespective of their business model.

At this important juncture in the policy debate on the future of EU consumer law, this CERRE Report takes a closer look at some of the key issues of a future DFA. In our report, we do not endeavour to address all issues that have been raised by the Commission in its public consultation. We would rather

[9] European Commission, 2030 Consumer Agenda, COM(2025) 848 final, p. 7.
[10] European Commission, Commission Work Programme 2026, COM(2025) 870, Annex I, p. 5.
[11] C Busch and A Fletcher, Harmful Online Choice Architecture, CERRE Report, May 2024.
[12] C Busch and A Fletcher, Shaping the Future of European Consumer Protection: Towards a Digital Fairness Act?, CERRE Issue Paper, December 2024.
[13] M Ledger, Protection of Minors: Age Assurance, CERRE Issue Paper, March 2025; M Buiten and C Busch, Protection of Minors: Age Appropriate Design, CERRE Issue Paper, March 2025; M Buiten and M Ledger, Charting the Path for the Protection of Minors Under the DSA, CERRE Issue Paper, March 2025.
[14] See e.g. M Grochowski, Consumer Law for a Post-Consumer Society, EuCML 2023, 1; M. Namyslowska, The Silent Death of EU Consumer Law and Ist Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices, Journal of Consumer Policy 2025, 317.

focus on some aspects that we consider to be particularly relevant for a future DFA that seeks to reconcile several policy issues: ensuring a high level of consumer protection in the digital environment and facilitating effective enforcement while promoting competitiveness and growth, which in turn requires avoiding over-regulation.

The report is structured as follows. Chapter 1 addresses several horizontal issues relating to overarching concepts and principles of consumer law and outlines three general principles for smart digital regulation. The following chapters zoom in on selected market practices and policy areas that the Commission seeks to address in the DFA. Chapter 2 focuses on issues with digital contracts and subscriptions. Chapter 3 analyses how the DFA could ensure a high level of protection of minors. Chapter 4 addresses addictive design features and other problematic features of digital products (e.g., in the video games sector). Finally, Chapter 5 takes a closer look at problematic personalisation practices.

1. Horizontal Issues

In its public consultation on the DFA, the Commission addressed not only focus areas (e.g., dark patterns, addictive design, personalisation practices, influencer marketing), but also 'horizontal issues' relating to overarching concepts and principles of consumer law. Following this approach, in this section, we first introduce three general principles for smart digital regulation that should guide policy interventions in the field of EU consumer law, and particularly the elaboration of a future DFA. We then zoom in on two of the 'horizontal issues' identified by the Commission, i.e. the introduction of a general 'fairness by design' obligation and the revision of the concepts of average consumer/ vulnerable consumer.

1.1 Three General Principles for Smart Digital Regulation

Building on earlier work of CERRE in the field of consumer law and digital regulation,[15] this section outlines three general principles for smart digital regulation that should guide the policy interventions in the various policy areas identified in the Digital Fairness Fitness Check. Smart digital regulation should be based on three general principles: (i) **risk-based regulation**; (ii) **design-based regulation**; and (iii) **ecosystem regulation**.

1.1.1 Risk-Based Regulation

First, regulation should address clearly identified problems only where they materialise and cause consumers harm, while not overburdening traders unaffected by those problems. This means that the DFA should differentiate between business models according to their specific risk profile. In this sense, the DSA could serve as a model, that imposes asymmetric due diligence obligations on different types of digital service providers depending on the nature of their services and the level of risk associated with their activities.[16]

From this perspective, the following questions should guide the elaboration of the DFA:

- What is the right scope of regulation? How to differentiate according to risk?
- Should the rules cover all product categories/services/digital content?
- Should the rules apply to all consumers/minors/vulnerable consumers?
- Should there be exceptions for SMEs/stricter rules for very large businesses?
- What is the appropriate regulatory instrument (opt-out, opt-in, total ban)?

[15] See e.g., A-L Sibony and A de Streel, Towards Smarter Consumer Protection Rules for the Digital Society, CERRE Report, October 2017; C Busch and A Fletcher, Harmful Online Choice Architecture, CERRE Report, May 2024; C Busch and A Fletcher, Shaping the Future of European Consumer Protection, CERRE Issue Paper, December 2024.
[16] European Commission, Proposal for a Digital Services Act, Explanatory Memorandum, COM(2020) 825, 6.

1.1.2 Design-Based Regulation

Second, consumer law should also follow a design-based approach. For effective consumer protection, it is not sufficient to enshrine consumer rights in legislation and to inform consumers about their rights. Rather, **the exercise of consumer rights must be facilitated by designing the user interfaces in such a way that consumers can easily exercise their rights.** An example of this regulatory approach is the recently introduced 'withdrawal button' (Art. 11a CRD).

From this perspective, the following questions should also be taken into account when drafting the rules of a future DFA:

- How can the design of user interfaces facilitate consumer choices (e.g., opt-out/opt-in) and the exercise of consumer rights (e.g., cancellation, withdrawal)?
- At which level of the 'digital stack' should the design-based solution be implemented (device level/browser/app store/individual app or website)?
- What level of detail should the design requirements have?
- Which design elements should be regulated in mandatory provisions and what could be included in guidances/codes of conduct? How to ensure technology-neutral design regulation? How to balance design-based regulation with giving traders the flexibility and freedom to differentiate and compete?

1.1.3 Ecosystem Regulation

Finally, the smart digital regulation should be based on an "ecosystem approach". B2C contracts are typically embedded in broader ecosystems with a variety of players. This means that policy interventions should look beyond the two-party relationship between the trader and the consumer and consider the different roles of the various actors in the respective "digital ecosystem" (e.g., app stores, online marketplaces, payment service providers). These players could play an important role as 'regulatory intermediaries'[17] and contribute to facilitating compliance and effective enforcement of consumer law.

From this perspective, the following questions should also be considered:

- Who are the relevant players in the respective digital ecosystem?
- What is their respective role and how do they interact with each other?
- How could roles and responsibilities be shared in the ecosystem?

[17] See more generally on regulatory intermediaries K W Abbott, D Levi-Faur and D Snidal, Theorizing Regulatory Intermediaries: The RIT Model, 670 The Annals of the American Academy of Political Science 14-35 (2017); see also C Busch, Self-regulation and regulatory intermediation in the platform economy, in: M Cantero Gamito and H-W Micklitz (eds), The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes, 2020, pp. 115-134.

1.2 Fairness by design

One of the horizontal issues raised for discussion in the public consultation on the DFA was whether traders should ensure 'fairness by design' (i.e., take technical and organisational measures to incorporate consumer protection considerations at all stages of the product or service development).[18] Similarly, the Commission's tender documents for the DFA Impact Assessment work mention as a possible policy measure "introducing a general 'fairness by design' obligation, possibly combined with a reversal/easing of the burden of proof in case of digital asymmetry/in technologically complex cases". [19]

The main idea behind the concept of "fairness by design" is that risks for consumers arising from choice architecture, algorithmic systems and personalisation mechanisms should be considered and mitigated already at the design stage. Such a design-based approach is not entirely new in EU law. Possible models include the concept of "privacy by design" (Art. 25 GDPR), "access by design" (Art. 3(1) Data Act), and "safety by design" (Art. 7(2)(a) Product Liability Directive).[20] Similarly, the risk assessment and risk mitigation requirements under Arts. 34 and 35 DSA applicable to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) could be seen as such a requirement.[21]

In practical terms, the concept of fairness by design could be implemented either as a new obligation for businesses or as an interpretative principle. As a **stand-alone obligation** a new legislative provision would require traders to engage in upfront "best efforts" to ensure their digital interfaces are "fair by design". It seems doubtful, however, how such a rather vague requirement could be enforced and how much added value such a provision would bring. Should the EU legislator decide to take this route, the new obligation would have to be accompanied by clear regulatory guidance for all market actors.

It therefore seems more convincing to introduce an **interpretative principle** of 'fairness by design'. Such an interpretative guidance could be linked to the concept of professional diligence. According to Art. 2(h) UCPD, 'professional diligence' means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity. This standard is referred to in Art. 5(2)(a) UCPD which states that a commercial practice is considered unfair if it is contrary to the requirements of professional diligence.

Building on this, the DFA should clarify that when assessing whether the standards of professional diligence have been met, choices made by the trader at the design stage should also be taken into account. However, when determining the specific requirements for traders at the design stage, the principle of proportionality must be taken into account. In particular, it must be ensured that SMEs are not excessively burdened.

[18] European Commission, Public consultation on the Digital Fairness Act, Factual Summary Report, December 2025, Ares(2025)11434262 - 19/12/2025, p. 18.
[19] Call for tenders EC-JUST/2024/OP/0001 (internal reference: JUST/2023/PR/JUH1/0096). https://ec.europa.eu/newsroom/just/items/820177/en.
[20] See also European Economic and Social Committee, Transport, energy and services of general interest as drivers of sustainable European growth through the digital revolution, Own-Initiative Opinion, 17.07.2019, TEN/691-EESC-2019, para. 2.8 (referring to the "principles of security and safety by design and by default").
[21] C Busch and A Fletcher, Harmful Online Choice Architecture, CERRE Report, May 2024, p. 29.

1.3 Concepts of Average/Vulnerable Consumer

In its final report on the Digital Fairness Fitness Check, the Commission states that "the provisions on the 'average consumer' and the 'vulnerable consumer' may need to be further clarified or amended to ensure effectiveness in the digital context".[22] Following up on this, the Commission suggests in the public consultation on the DFA and the tender documents for the DFA Impact Assessment work that the current concepts of average consumer/vulnerable consumer could be revised.[23]

1.3.1 Average consumer

Currently, the main benchmark for the application and interpretation of EU consumer law is the concept of the "average consumer" (Art. 5(2) UCPD), defined in Recital 18 UCPD as being "reasonably well informed and reasonably observant and circumspect". This normative concept, which was initially developed by the CJEU,[24] has long been criticised by research on consumer behaviour as a somewhat unrealistic assumption.[25] Similarly, in its final report on the Digital Fairness Fitness Check, the Commission states that "the growing mismatch between the normative abstract of the 'average consumer' and the realities of consumer behaviour in the digital environment undermines the effectiveness of EU consumer law".[26]

More recently, in its ***Compass Banca*** decision, the CJEU underlined that the average consumer test is not "supposed to be merely a theoretical exercise" and that "considerations that are more realistic must also be taken into account".[27] More specifically, the Court held that "the fact that the concept of 'average consumer' must be understood by reference to a consumer who is 'reasonably observant and circumspect' does not exclude taking into account the influence of cognitive biases on that average consumer, provided that it is established that such biases are likely to affect a reasonably well-informed and reasonably observant and circumspect person, to such an extent as to materially distort his or her behaviour."[28] In a sense, the *Compass Banca* decision, "reflects a growing judicial sensitivity to the cognitive limitations that affect real-world decision-making".[29] At the same time, the decision shows that the concept of the 'average consumer' is flexible enough to also take behavioural insights and situational aspects into account. **Against this background, it does not appear necessary to fundamentally revise the current consumer benchmark. As a matter of clarification, it could be helpful, however, to codify the more recent case law of the CJEU,** for example, in the recitals of the DFA.

[22] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*. SWD(2024) 230 final, p. 48.
[23] European Commission, Public consultation on the Digital Fairness Act, Factual Summary Report, December 2025, Ares(2025)11434262 - 19/12/2025, p. 18; see also Call for tenders EC-JUST/2024/OP/0001 (internal reference: JUST/2023/PR/JUH1/0096). https://ec.europa.eu/newsroom/just/items/820177/en.
[24] CJEU, Case C-210/96 Gut Springenheide and Rudolf Tusky v Oberkreisdirektor des Kreises Steinfurt [1998] ECR I – 4657, paras 30-31.
[25] See, e.g., Rossella Incardona & Cristina Poncibò, The average consumer, the unfair commercial practices directive and the cognitive revolution, 30 Journal of Consumer Policy 21 (2007); see also Hanna Schebesta & Kai P. Purnhagen, Island or Ocean: Empirical Evidence on the Average Consumer Concept in the UCPD, 28 European Review of Private Law 293-310 (2020). For a more general overview see Fabrizio Esposito, Conceptual foundations for a European consumer law and behavioural sciences scholarship in Hans-W. Micklitz, Anne-Lise Sibony & Fabrizio Esposito (eds) Research Methods in Consumer Law (Edward Elgar Publishing 2018) 38-76.
[26] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*. SWD(2024) 230 final, p. 46.
[27] CJEU, Case C-646/22 Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato (Nov. 14, 2024), para. 51.
[28] Id. At para. 53.
[29] T Ngamsanguan, Digital Fairness, Algorithmic Manipulation and Behavioural Exploitation in the EU: A Universal Vulnerability-Informed Critique of Consumer Protection in the Digital Services Act, EuCML 2025, 325 at 328.

1.3.2 Vulnerable consumer

Art. 5(3) UCPD refers to the concept of the 'vulnerable consumer' who is particularly vulnerable due to characteristics such as their mental or physical infirmity, age or credulity.[30] According to a growing strand of literature, consumer vulnerability should no longer be considered as a group-based concept referring to personal characteristics. Rather, in digital environments, consumer vulnerability should be understood as a structural or systemic phenomenon resulting in particular from the design of digital choice architectures (**"digital vulnerability"**).[31]

It is indeed increasingly difficult to draw categorical distinctions between 'average' and 'vulnerable' consumers, particularly in digital contexts. Even consumers who do not suffer from 'mental or physical infirmity' or 'credulity' encounter structural asymmetries in digital environments that can make them vulnerable to specific forms of (algorithmic) manipulation. However, this should not lead to the conclusion that all consumers are "vulnerable consumers" in digital environments. This would undermine the concept and render it legally irrelevant. Rather, **the systemic and situational aspects of "digital vulnerability" should be taken into account when applying the "average consumer" concept**, as explained above.

Additionally, the Commission also emphasises that the vulnerability characteristics highlighted in the UCPD form a non-exhaustive list and that the concept can be interpreted in a dynamic and situational manner.[32] Thus, the concept of vulnerability may include "context-dependent vulnerabilities that are particularly acute in a digital environment characterised by data collection on socio-demographic characteristics but also personal or psychological characteristics, such as interests, psychological profile and mood".[33] For example, in section 4, we discuss the need to protect consumers who tend towards addictive behaviour. In this sense, there is a fluid transition between the concept of the 'average consumer' and that of the 'vulnerable consumer'. **This flexible and dynamic interpretation of "vulnerability" should be codified in the DFA.** This approach can and should be combined with a **group-based understanding of 'vulnerability'**. In particular, the DFA should focus on the vulnerabilities of minors who are active in the digital environment. Currently, the UCPD mainly applies the concept of vulnerability as an interpretative standard that serves as a benchmark for assessing a certain commercial practice. In contrast, in the DSA, the specific vulnerabilities of minors constitute a concrete legal element of regulation (see e.g., Art. 28 DSA). The DFA could follow this model and introduce specific protection standards for minors, e.g., with regard to addictive design or personalisation practices (see Chapters 4 and 5).

[30] See also Recital 19 UCPD and Recital 34 CRD.
[31] For an overview, see Camilla Crea and Alberto De Franceschi (eds), The New Shapes of Digital Vulnerability in European Private Law (Nomos 2024); see also Natali Helberger, Betül Kas, Hans-W. Micklitz, Monika Namysłowska, Laurens Naudts, Peter Rott, Marijn Sax, Michael Veale, Digital Fairness for Consumers, BEUC Report (May 2024), p. 12 (arguing that the concept of digital vulnerability is 14haracterised by three aspects, "its relational nature, its architectural nature, and the erosion of privacy"). Other authors refer to "systemic vulnerability", see e.g., Christine Riefa, Protecting vulnerable consumers in the digital single market, (2022) European Business Law Review, 33, 607-634 (arguing that consumer vulnerability is created by the system design, in particular the design of online choice architectures).
[32] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*. SWD(2024) 230 final, p. 47.
[33] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*. SWD(2024) 230 final, p. 47.

2. Digital Contracts

2.1 Introduction

In its final report on the Digital Fairness Fitness Check, the European Commission identifies several issues regarding digital contracts and subscriptions, such as difficulties with cancelling contracts online, automatic renewals, and the conversion of free trials into paid subscriptions.[34] According to the Commission, "EU consumer law cannot be considered effective in addressing the concerns regarding digital contracts and subscriptions, including specifically their cancellation and renewal".[35] The Commission also criticises the increasing regulatory fragmentation caused by the growing number of national regulations for subscriptions.

The Commission is proposing to address these concerns through the forthcoming DFA. In this section, we first consider the rationale for regulating in this area, why it matters, and the extent to which existing regulation addresses the identified concerns. We then discuss the Commission's possible policy measures relating to digital contracts.

2.2 The Rationale for Regulation in this Area

2.2.1 Concerns regarding digital contracts

In recent years, subscription models have become increasingly popular across various sectors of the consumer economy. According to some estimates, the size of the subscription economy has quadrupled over the last decade.[36] Subscriptions are now available for almost everything, including news services, video and music streaming, meal kits, fitness apps and additional features for apps such as online dating. It is important to note that the subscription economy is not a monolithic bloc, but rather characterised by a variety of products and services, consumption patterns, pricing models, billing methods and distribution channels.[37]

From a consumer perspective, subscriptions offer convenience and continuity, and they can help to reduce transaction costs for recurring use of goods or services. For businesses, subscription models provide a reliable source of revenue and the possibility to generate detailed data about consumption habits and customer preferences. However, the shift from one-off purchases to subscriptions also creates new risks for consumers. We know from behavioural research that consumers may suffer from inattention, inertia and overoptimism. As a result, consumers often forget to cancel subscriptions that they no longer use and end up "paying not to go to the gym".[38] In addition, some businesses may use

[34] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*. SWD(2024) 230 final.
[35] European Commission (n. 9), 182.
[36] L Einav, B Klopack, and N Mahoney, *Selling Subscriptions*. NBER Working Paper 31547, August 2023, <http://www.nber.org/papers/w31547> (all websites last accessed 1 November 2024), 1; see also T Chen, K Fenyo, S Yang, and J Zhang, *Thinking inside the subscription box: New research on e-commerce consumers*. (McKinsey & Company, February 2018), 1 (estimating that the subscription e-commerce market has grown by more than 100 percent a year between 2013 and 2018).
[37] See, generally, T Rudolph, SF Bischof, TM Böttger, and N Weiler, 'Disruption at the door : a taxonomy on subscription models in retailing' (2017) 34 Marketing Review St. Gallen 18; see also SF Bischof, TM Böttger, and T Rudolph, 'Curated subscription commerce: A theoretical conceptualization' (2020) 54 Journal of Retailing and Consumer Services 101822.
[38] S Della Vigna and U Malmendier, Paying Not to Go to the Gym, 96 American Economic Review 694-719 (2006).

design features to make cancelling subscriptions unduly difficult.[39] This is not only a problem from a consumer protection perspective but could also hamper competition among providers of subscription services or drive competition in directions that are not actually in consumers' interests.

2.2.2 Is there a Regulatory Gap?

There are a number of pieces of EU legislation that are relevant to the subscription economy. However, the current regulatory framework at EU level remains fragmented and contains a number of gaps.

Consumer Protection Law

The existing EU consumer contains several provisions that address issues with digital contracts and subscriptions. For example, Art. 5(1)(f) and Art. 6(1)(o) CRD stipulate transparency requirements regarding duration of contract and conditions for terminating the contract.[40] In addition, Art. 5 UCTD requires the relevant contract terms to 'be drafted in plain, intelligible language'. Moreover, withdrawing from a subscription contract should become easier as the recently added Article 11a of the Consumer Rights Directive requires traders to provide a prominently displayed and easily accessible "withdrawal function". Furthermore, in the UCPD Guidance, the Commission underlines that cancellation must be as simple as sign-up and creating barriers to contract termination can be regarded as an aggressive practice under Art. 9(d) UCPD.[41]

Digital Services Act and Digital Markets Act

More recently, the EU Digital Rulebook has added further provisions that are relevant for digital subscriptions. Article 25 DSA prohibits online platforms from manipulating users or otherwise distorting their ability to make free and informed decisions, including by making it more difficult to terminate a service than subscribing to it.[42] Furthermore, Art. 6(13) DMA precludes gatekeepers from imposing disproportionate conditions for terminating the provision of a core platform service and mandates that any conditions for termination can be exercised without undue difficulty.

Sector-Specific Rules

Apart from the above-mentioned provisions, EU law does not contain any horizontal provisions that expressly regulate automatic renewals, reminders, the change from a free trial to a paid-for subscription and the provision of payment details to start a free trial.[43] However, there are some examples of sector-specific rules that apply to certain categories of subscription contracts. In particular, the European Electronic Communications Code (EECC) contains specific rules regarding the duration of contracts for electronic communication services.[44] According to Art. 105(1) EECC, fixed-term contracts for electronic communication services must not mandate a commitment period longer than 24 months. Member States are free to stipulate even shorter maximum periods. In addition,

[39] For example, the FTC has taken action against Amazon alleging that the company used deceptive methods to sign up consumers for Prime subscriptions and made it exceedingly difficult to cancel. In September 2025, the FTC secured a settlement in the case.
[40] European Commission, Digital Fairness Fitness Check, Final Report, p. 179.
[41] European Commission, UCPD Guidance, 2021, p. 60.
[42] The Commission may issue guidelines which cover the cancellation of subscriptions to an online platform service, Art.25(2)(c) DSA.
[43] European Commission, Digital Fairness Fitness Check, Final Report, p. 180.
[44] Art. 105(1) EECC specifies that this provision does not apply to number-independent interpersonal communications services and other than transmission services used for the provision of machine-to-machine services.

Article 105(3) EECC requires providers to send their customers a reminder before the contract is automatically renewed. This must be done in a prominent and timely manner and via a durable medium at the end of the contractual commitment and state the means for terminating the contract. Additionally, Art. 105(3) EECC stipulates that after automatic renewal of the contract, customers are entitled to cancel the contract at any time with a short notice period (one month) and without incurring any costs except the charges for receiving the service during the notice period.

Another example of a sector-specific rule that is relevant for subscriptions is the recently introduced Art. 16e CRD which contains a prohibition of dark patterns. The provision, which applies only to financial services contracts concluded at a distance, explicitly bans traders from "making the procedure for terminating a service more difficult than subscribing to it" (Art. 16e(1)(c) CRD). The provision thus corresponds verbatim to Art. 25(3)(c) DSA.

Increasing Regulatory Activity at Member State Level

While EU consumer law still focuses very much on one-off purchases ("sale paradigm"), several national legislators have recently introduced specific rules on subscription contracts.[45] For example, in March 2022, Germany tightened the rules for automatic renewals of subscriptions and introduced a "cancellation button".[46] Similarly, in August 2022, France added provisions to its Consumer Code to make it easier for consumers to cancel subscription contracts.[47] In Italy, in 2023 a new provision was introduced into the Consumer Code which requires traders to send a reminder 30 days before renewal applies only to service contracts (including digital services).[48] In addition, the new Spanish Law 10/2025 requires companies to notify consumers at least 15 days in advance of the date of the automatic subscription renewal.[49] The proliferation of such regulations at Member State level creates a growing risk of regulatory fragmentation across the EU.

2.3 The Commission's Possible Policy Measures

In this section, we first describe general principles for policy intervention in the field of digital contracts and subscriptions, and then discuss how the Commission's list of "possible policy measures" fits with these general principles.

2.3.1 General Principles for Policy Intervention

As briefly outlined in the section on horizontal issues, smart digital regulation should be based on three general principles: (i) risk-based regulation; (ii) design-based regulation; and (iii) ecosystem regulation. This section briefly explains how these principles can be applied in the subscription economy.

[45] See e.g., K Caruso and P Cox, 'Silence as Consumer Consent: Global Regulation of Negative Option Contracts' (2024) 73 American University Law Review 1611; see also C Busch, 'Updating EU Consumer Law for the Digital Subscription Economy' (2022) 11(2) EuCML 41.
[46] Gesetz für faire Verbraucherverträge (10 August 2021), Bundesgesetzblatt 2021 I 3433.
[47] Loi n° 2022-1158 du 16 août 2022 portant mesures d'urgence pour la protection du pouvoir d'achat, art. 17, 18; see G Loiseau, 'La résiliation des contrats par voie électronique, (2022) 12 Communication Commerce Electronique 28; see also T Douville, 'La résiliation par voie électronique', (2022) 32 Recueil Dalloz 1602.
[48] Article 65-bis Codice del consumo. The provision was introduced by Article 14 of Law n. 214/2023 of 30 December 2023 (Annual Law for the Market and Competition 2022).
[49] Ley 10/2025, de 26 de diciembre, por la que se regulan los servicios de atención al clientela.

Risk-Based Regulation

First, the regulation of subscriptions should be risk-based and differentiate between business models according to their specific risk profile. In other words, future EU rules for subscriptions should target specific risks and associated consumer harms and treat them proportionally:

- **Distinction between different categories of products:** For example, risks caused by inattention and inertia are rather high in contracts for services and digital content (e.g., streaming services, cloud storage). In contrast, the risk that consumers will simply forget their subscription in the case of weekly or monthly deliveries of physical products (e.g., meal boxes, printed newspapers or magazines) is lower. An example of risk-based regulation is provided by Art. 65-*bis* of the Italian Consumer Code, which requires traders to send a reminder 30 days before renewal applies only to service contracts (including digital services).
- **Differentiation according to the duration of the contract renewal:** Another factor that could be taken into account in the risk analysis is the duration of the contract renewal. The longer the consumer is 'locked in' to the contract upon renewal, the greater the risk for the consumer. Accordingly, the degree of regulation could be graded according to the length of the contract renewal. For example, one could ask whether requirements for reminders before automated renewal should depend on the duration of contract renewal (e.g., only for contracts that are renewed for more than 3/6/12 months).

Design-Based Regulation

Second, the regulation of subscriptions should also follow a design-based approach. For some time now, there has been a trend in European consumer law and digital law away from 'information-based regulation' towards 'design-based regulation'. Whereas in the past, the provision of information was considered crucial to protecting consumer autonomy, more recently the focus has shifted to the design of user interfaces. This is evidenced by the numerous regulations dealing with manipulative designs ('dark patterns').[50]

There are two different categories of design-based rules:

- **"Negative" design rules** that prohibit certain harmful design choices (e.g., the use of dark patterns or manipulative online choice architectures). Examples of this regulatory approach are Art. 25 DSA, Art. 6(13) DMA and Art. 16e CRD. These rules leave more freedom of choice for online interface designers, however at the price of less legal certainty.
- **"Positive" design rules** that prescribe certain design choices that are beneficial for consumers (e.g., by enabling consumers to easily exercise their rights). Examples of the "positive" approach to consumer protection by design are the cancellation buttons recently introduced by legislators in Germany (§ 312k German Civil Code) and France (Art. L-215-1-1(2) French Code Consumer Code) and the recently introduced withdrawal function (Art. 11a CRD). These rules restrict freedom of design choices to higher degree, but they have the advantage of offering businesses, consumers and authorities more legal certainty. In addition, they tend to promote consistency across different services and make it easier for consumers to navigate

[50] For an overview see C Busch and A Fletcher, Harmful Online Choice Architecture, CERRE Report, May 2024; see also M Leiser, Dark Patterns, Deceptive Design and the Law, 2025.

their choices.

Ecosystem Regulation

Finally, the regulation of subscriptions should be based on an "ecosystem approach". This means that future EU rules on subscriptions should not be limited to the two-party relationship between traders and consumers. A more holistic approach is preferable, which also involves the other players within the subscription ecosystem as **regulatory intermediaries**.[51]

In this perspective, the Commission should give thought to the responsibilities of other actors in the "**subscription stack**" (e.g., app stores, online marketplaces as well as providers of payment services and subscription management tools). In this context, it is important that the division of obligations and responsibilities are clear. Operators of app stores and online marketplaces, payment service providers and providers of subscription management tools should each make their own contribution to consumer protection in the subscription economy. This also seems justified from an economic point of view, since in many cases they can be regarded as the cheapest cost avoider.[52]

- For example, following the model of Art. 31 DSA, providers of app stores and online marketplaces could be required to **make best efforts** to assess whether third-party providers of subscription-based services have the necessary design features in place to comply with consumer law requirements (e.g., cancellation button, reminders before renewal).
- Similarly, providers of subscription management tools could be required to ensure that their software tools are in compliance with consumer law rules for subscriptions (e.g., cancellation button, reminders before renewal).

2.3.2 The Commission's Possible Policy Measures

Having set out the general principles for regulation of digital contracts, we now consider the Commission's list of "possible policy measures", as set out in the Commission's tender documents for the DFA Impact Assessment work (under Topic 6).[53] At the time of writing, it is unclear how finalised these are, but they can serve as a starting point for discussion here. The following table provides an overview of the measures that are currently being considered by the Commission:

Measure 1	Introduction of an easy cancellation facility ('button') for consumers on sites/applications enabling the conclusion of contracts online (like the facility for the exercise of the right of withdrawal that has been recently introduced in the CRD).

[51] See more generally on regulatory intermediaries K W Abbott, D Levi-Faur and D Snidal, Theorizing Regulatory Intermediaries: The RIT Model, 670 The Annals of the American Academy of Political Science 14-35 (2017); see also C Busch, Self-regulation and regulatory intermediation in the platform economy, in: M Cantero Gamito and H-W Micklitz (eds), The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes, 2020, pp. 115-134.
[52] C Busch and C Twigg-Flesner, A Roadmap for Regulating Subscriptions in the Digital Fairness Act, 13 Journal of European Consumer and Market Law 234-241 (2024).
[53] Call for tenders EC-JUST/2024/OP/0001 (internal reference: JUST/2023/PR/JUH1/0096). https://ec.europa.eu/newsroom/just/items/820177/en.

Measure 2a	Possibility to terminate the automatically extended subscription any time with short (one month) notice (similar to what exists under the Electronic Communications Code).
Measure 2b	Reminder before a subscription is automatically renewed or a free trial is converted into a paid subscription: (i) for all contracts or (ii) only for digital subscriptions (not for physical goods).
Measure 2c	Measure 2b, coupled with the requirement that the consumer should actively accept the renewal or conversion: (i) for all contracts or (ii) only for digital subscriptions (not for physical goods).
Measure 3:	Right of access to a human interlocutor in consumer services.

Easy Cancellation Facility

Measure 1: Introduction of an easy cancellation facility ('button') for consumers on sites/applications enabling the conclusion of contracts online (like the facility for the exercise of the right of withdrawal that has been recently introduced in the CRD)

At the top of the Commission's list of possible policy measures regarding digital contracts and subscriptions is the introduction of an 'easy cancellation facility' which is broadly modelled on the cancellation buttons recently introduced in Germany and France, for example. As a 'positive' design rule, the measure would make it easier for consumers to exercise their termination rights.

When drafting the technical details of an 'easy cancellation facility', the EU legislator should take into account the experience gained with similar regulations in France and Germany. Recent case law regarding the German cancellation button (§ 312k German Civil Code) indicates that vaguely formulated design requirements ("easily accessible") should be avoided in order to ensure legal certainty.[54] Another option would be to supplement broadly formulated design requirements with more specific guidelines in delegated acts/guidance documents (e.g., placement of cancellation button in the footer of a website).

Another practical question to be addressed in a future EU regulation is the extent to which customer retention attempts (so-called "saves") should be permitted as part of the termination process. Traders often offer consumers who are about to cancel their subscription a special discount to keep them on board.[55] Sometimes, customers are also offered the option to pause instead of terminating their subscription. Whether these are treated as dark patterns that make termination more difficult, or legitimate measures that offer the consumer a good deal, might not be easy to identify, and legislative clarification will be needed to avoid overlaps with existing rules, in particular the UCPD.

[54] See e.g., Kammergericht, 21.01.2025, Case 5 UKl 8/24.
[55] See e.g., OLG Düsseldorf, 18.09.2025, Case 20 Ukl 1/25.

Moreover, the first reported cases regarding cancellation buttons at Member State level suggest that some providers will most likely seek ways to circumvent such a future EU rule requiring a cancellation facility. The Commission should therefore consider supplementing the design-based rule with an anti-circumvention rule for which Art. 13 DMA could serve as a model.[56]

Possibility to Terminate the Automatically Extended Subscription at any Time with Short Notice

Measure 2a: Possibility to terminate the automatically extended subscription any time with short (one month) notice (similar to what exists under the Electronic Communications Code)

This provision is modelled on Article 105(3) EECC, which, however, only applies to contracts for electronic communication services. In contrast, the new provision would apply to all types of contracts. At Member State level, there are already comparable provisions with a broad scope of application (e.g., Section 309 No. 9 lit. b German Civil Code) which would be superseded by the new EU regulation.

The provision would reduce the risk of consumer lock-in, as the consumer can terminate the contract at short notice after it has been automatically renewed. However, the provision does not solve the problem that some consumers simply forget about their subscription.

Furthermore, the question arises as to how this provision will interact with the planned rules on reminders (Measure 2b). Is the renewed contract a contract of indeterminate duration? If so, there would be no renewal and, as a consequence, no reminder. Alternatively, one could assume that the contract is renewed every month for a further month. In this case, a reminder would have to be sent every month, which is also not reasonable. To solve this problem, one could consider supplementing the provision to the effect that a reminder is sent after certain time periods (e.g., 6 months, 12 months).

Reminder Before Automatic Renewal or Conversion

Measure 2b: Reminder before a subscription is automatically renewed or a free trial is converted into a paid subscription: (i) for all contracts or (ii) only for digital subscriptions (not for physical goods)

Measure 2b envisages the introduction of reminders prior to automatic renewal or conversion of a free trial into a paid subscription. A comparative legal survey shows that mandatory reminders before automatic renewal of subscription contracts are a frequently used regulatory tool.[57] Such reminders are particularly useful in cases where the automatic renewal leads to a long commitment period (e.g., six or twelve months). As already mentioned, at EU level, there is currently no horizontal rule that requires traders to send consumers a reminder prior to auto-renewal. The planned regulation takes the sector-specific regulation in Article 105 EECC as a model and extends it to other types of contracts.

[56] According to Art. 13(4) DMA, "gatekeeper shall not engage in any behaviour that undermines effective compliance with the obligations of Articles 5, 6 and 7 regardless of whether that behaviour is of a contractual, commercial or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design."

[57] See e.g., K Caruso and P Cox, 'Silence as Consumer Consent: Global Regulation of Negative Option Contracts' (2024) 73 American University Law Review 1611; see also C Busch and C Twigg-Flesner, A Roadmap for Regulating Subscriptions in the Digital Fairness Act, 13 Journal of European Consumer and Market Law 234-241 (2024) at 237.

As regards the scope of the provision, the EU legislator should consider the different risk profiles of the various subscription business models. Reminder notices do not seem necessary for short-term contracts involving the regular supply of physical goods (e.g., meal kits, beauty boxes). In these cases, the risk of consumers forgetting their subscription is rather low, as the physical goods themselves act as a reminder. In contrast, as already mentioned, there is a greater need for reminders in the case of contracts for services and digital content. This distinction is also reflected by the recently introduced Art. 65-*bis* of the Italian Consumer Code which requires traders to send a reminder 30 days before renewal applies only to service contracts (including digital services).[58]

When drafting the rule, the EU legislator should take into consideration that the effectiveness of the reminder depends on its timeliness. The consumer should receive the reminder neither too early nor too late.[59] The comparative analysis shows that the rules on notice periods differ considerably.[60] Art. 105(3) EECC does not specify an exact time period, but merely stipulates that the reminder must be provided "in a prominent and timely manner".[61] This might not be a good model for potential EU rules on reminders generally because of its inherent vagueness and lack of legal certainty.

An innovative approach would be to regulate the exact time window for sending the reminder not in the DFA itself, but in a delegated act that could be more easily adapted. This would enable the Commission to adapt the notice periods for reminders and determine the optimal timing based on empirical findings.

Active Acceptance Before Automatic Renewal or Conversion

Measure 2c: Measure 2b, coupled with the requirement that the consumer should actively accept the renewal or conversion: (i) for all contracts or (ii) only for digital subscriptions (not for physical good)

Measure 2c goes beyond the obligation to send reminders and adds a requirement that the consumer actively accepts the renewal or conversion. This would effectively eliminate the possibility of 'automatic' renewal or conversion.

At first glance, this measure seems to ensure a particularly high degree of consumer autonomy. However, it comes with considerable risks for consumers. One advantage of subscriptions with auto-renewal is precisely that consumers do not have to actively take care of contract renewal. This advantage would be lost if consumers had to actively accept the renewal in order to keep their contract. In such a scenario, inattention and inertia on the part of the consumer would result in losing the contract. This can have significant disadvantages for consumers, especially in the case of important contracts (such as insurance contracts). This effect is probably less serious in the case of free trial that is converted into a paid subscription. Therefore, Measure 2c should be considered, only in these cases, if at all.

[58] Art. 65-bis Codice del consumo, Law n. 214/2023.
[59] A Fletcher et al., 'Consumer Protection for Online Markets and Large Digital Platforms' (2023) 40 Yale Journal on Regulation 875, 898.
[60] For example, in California reminders must be given at least 15 days and not more than 45 days before the automatic renewal (Cal. Bus. & Prof. Code. § 17602(b)(2)). In Illinois, the notice period is between 30 and 60 days before auto-renewal (815 Illinois Comp. Stat. 601/10).
[61] Some authors argue that Art. 105(3) EECC requires traders to send the reminders out at least two weeks before the end of the cancellation period, see N Lueg in H Gersdorf and BP Paal (eds.) *BeckOK Informations- und Medienrecht*, 42nd edition, (Beck, 2023), § 56 TKG para. 8.

Right of Access to a Human Interlocutor

Measure 3: Right of access to a human interlocutor in consumer services

At first glance, the last measure in the Commission's list does not seem to fit in with the rest of the measures. It does not concern the termination or renewal of subscriptions, but rather the communication between the parties of a consumer contract. However, effective communication is more important in contracts of a certain duration, such as subscriptions, than in one-off transactions. Therefore, the regulation is indeed related to subscriptions, but is of broader relevance.

The question of a right of access to a human interlocutor has recently become increasingly important, as more and more businesses are automating their customer communication and replacing human agents in call centres with chatbots or AI agents. For simple and straightforward questions, a chatbot available 24/7 may be a convenient solution for consumers. However, when it comes to more complicated issues, many consumers (especially older ones) may want to speak to a human interlocutor. In principle, this seems justified. More recently, the EU legislator has reacted to this development by enacting Article 16d(3) CRD, which grants consumers a right to request and obtain human intervention. However, the sector-specific provision only applies to financial services contracts concluded at a distance.

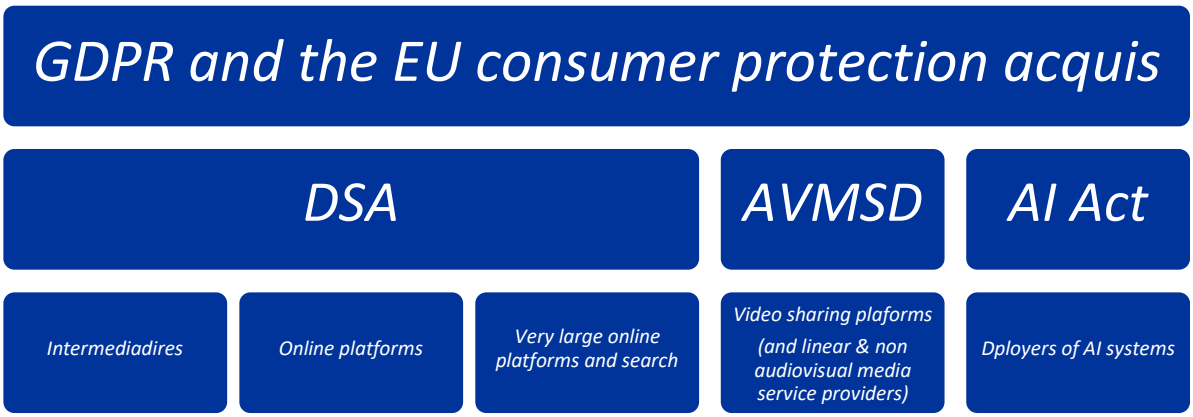
The proposed Measure 3 raises numerous practical questions. What exactly does 'right of access to a human interlocutor' mean? Does the trader have to provide a hotline between 12:00 and 14:00 h? Or is 24/7 human customer service required? The latter would place a considerable burden on start-ups and SMEs in particular. Does the trader have to provide 'direct' access to the human interlocutor? Or can a chatbot be used as a first point of contact? The proposal for the DFA will have to answer these questions. In view of the principle of proportionality, it might make sense to introduce such a right of access only for contracts above a certain financial volume.

3. Protection of Minors

The need to protect the online lives of children is at the forefront of recent debates in Brussels, and also in some Member States and in other regions of the world. Some jurisdictions, including the EU, are discussing banning children from accessing social media (and other services). The Commission has announced the setting up of a panel of experts to assess the need for an EU approach to digital age limits and which online services should be covered.[62]

This section focuses on the EU-level rules on the protection of minors and if and how the DFA could contribute to increasing their protection online, without complexifying an already complicated situation. Without going into the pros and cons of introducing a potential ban on access to children to social media or to other services it also addresses whether this should be addressed in the DFA and whether the instrument could cover age assurance.

There are some EU level rules that seek to protect minors online. Some of these are general in nature, leaving service providers to decide on what measures they should take, and sometimes giving the Member States the ability to introduce more far-reaching rules to protect minors. Another layer of complexity is that some of the legal instruments have a horizontal scope of application (they apply to all services) and while others have a sector specific scope of application (only some services are in scope). The situation is illustrated in the following visual.



3.1 Horizontal Rules on the Protection of Minors: GDPR and the Consumer Protection Acquis

Article 8 of the General Data Protection Regulation (GDPR) provides that **when data processing is based on consent**[63] and when online services are directly offered to children, the processing is lawful where the child is at least 16 years old. If the child is below 16 years, consent should be given or

[62] Ursula von der Leyen, State of the Union Address, 10 September 2025, available at https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_25_2053.

[63] In many cases, data controllers opt for other legal basis than consent to process the personal data of minors, such as the execution of a contract or legitimate interest (Policy Brief, Mind the Gap, Age Assurance and the Limits of Enforcement under EU Law, Jessica Galissaire, October 13, 2025 available at https://www.interface-eu.org/publications/age-assurance-gap).

authorised by the holder of parental responsibility. However, the Member States may set a lower age for when children can begin to give consent, if it is not below the age of 13.[64]

Article 8 therefore puts quite a bold limit on processing data of minors without the consent of holders of parental responsibility. If this provision was enforced properly, far less children would probably be present online and online services would most probably not be allowed to engage in addictive design features based on the profiling of minors. This article is key to the protection of minors online.

3.1.1 The Consumer Protection Acquis and the Concept of Vulnerable Consumer

Except for the UCPD, EU consumer protection legislation does not contain child specific rules, although as general horizontal rules, they also serve to protect minors in their transactional relationship with traders.

The UCPD prohibits misleading or aggressive practices that could materially distort the economic behaviour of an average consumer. Article 5(3) UCPD recognises that children are 'vulnerable consumers' but does not attach a direct consequence to that fact, for instance by stating that traders need to be particularly mindful of not exploiting their vulnerability. Instead, the article states that commercial practices that are likely to materially distort the economic behaviour **only of a clearly identifiable group of consumers who are particularly vulnerable** to the practice or the underlying product **because of their** mental or physical infirmity, **age** or credulity **in a way which the trader could reasonably be expected to foresee**, ***need to be assessed from the perspective of the average member of that group***. The UCPD also refers to the concept of **targeted average consumer.** If a commercial practice targets a certain group of consumers, then the practice needs to be evaluated from the average member of that specific group.

3.2 Sector Specific Rules on the Protection of Minors: Audiovisual Media Services Directive, the DSA and the AI Act

According to Article 28b Audiovisual Media Services Directive[65] (AVMSD), **Video-Sharing Platforms** (VSPs) **need to put in place "appropriate measures"** to protect minors from content that could impair their physical, mental or moral development. The article lists possible appropriate measures such as age verification, parental controls and age ratings. The Member States are free to introduce more far-reaching rules in relation to VSPs established in their territories since the AVMSD is a minimum harmonisation directive.

Concerning linear and on-demand audiovisual media services, Article 6a AVMSD provides that **Member States should ensure** that services provided by media service providers under their

[64] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation.

[65] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, OJ L 303, 28.11.2018, pp. 69–92.

jurisdiction which may impair the physical, mental or moral development of minors should only be made available in such a way that minors will not normally hear or see them. Proportionality is brought into the provision since the measures taken (such as watersheds; age verification or other technical measures) should be proportionate to the potential harm of the programme. The most harmful content, such as gratuitous violence and pornography, should be subject to the strictest measures. Further the Article 6a also specifies that personal data of minors collected or otherwise generated by media service providers to protect them cannot be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising. Member States have adopted detailed rules to implement Article 6a AVMSD at the national level. It is also interesting to note that the aim of this provision is to protect minors from a broad range of harms since the article refers explicitly to the need to protect them from services that could impair their physical, mental and moral development.

The DSA also contains a number of specific rules to protect minors:

- Article 14 DSA obliges all intermediaries to specify any restrictions they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions (T&C). They should also act in a diligent, objective and proportionate manner in applying and enforcing T&C with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service. Where an intermediary service is primarily directed at minors or is predominantly used by them, providers of intermediary services need to explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand;
- Article 28 (1) DSA according to which online platforms (such as social media, video-sharing platforms, app stores and marketplaces- but not online search engines and not online platforms that qualify as small and microenterprises) that are accessible to minors must take appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors. The Commission has issued guidelines to help online platforms comply with this part of Article 28 (see table 1 below);
- Article 28 (2) DSA provides that online platforms cannot present advertisements based on profiling (as defined in the GDPR) by using the personal data of minors (to the extent that they are aware, with reasonable certainty, that they are minors);
- Articles 34 and 35 whereby the online platforms (and search engines) designated by the Commission as very large (active monthly EU users above 45m) must annually assess negative effects of their services for the protection of minors, the rights of the child, and serious negative consequences for their physical and mental well-being, and mitigate any identified systemic risk. The list of possible mitigation measures they need to deploy includes age verification, parental control tools and tools to help minors signal abuse or to obtain support. The Commission has announced on multiple occasions that it is prioritising the enforcement of the rules on the protection of minors of the DSA. It is carrying out investigations into some of the VLOPS (adult platforms[66] - for not putting in place age verification tools; online

[66] Commission press release of 27 May 2025, investigations into Pornhub, Stripchat, XNXX and XVideos, avalable at https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1339.

marketplaces -[67]; and social networks). On 18 June 2025, the EU Commission accepted and made legally binding a set of commitments offered by AliExpress to address multiple breaches of the DSA[68]. One such commitment relates to putting in place a system by default to limit visibility of products intended for adults (e.g., automatically blurring images of adult products using AI-powered real-time scanning technology). In August 2024, the Commission also accepted commitments by TikTok to permanently withdraw its Lite Rewards programme from the EU and to not launch a similar programme[69]. The Commission found that TikTok was in breach of articles 34 and 35 DSA because it failed to conduct risk assessment on actual or foreseeable harms to the physical and mental health of users, given the "multiple problematic design patterns to retain users on the service ; to include in the risk assessment, actual or foreseeable harms for the rights of the child and in relation to the protection of minors; and to take effective measures to mitigate risks that should have been identified. In relation to other social media, the Commission has also opened formal proceedings against Facebook and Instagram on the grounds that their algorithms may be stimulating addictive behaviour in children while also creating rabbit hole effects, and that they are failing to put in place appropriate mitigation measures to prevent access by minors to inappropriate content, notably age verification tools.[70]

Finally, Article 5 of the AI Act prohibits systems that exploit age-related vulnerabilities or the use of manipulative or subliminal techniques.

Table 1 Overview of Commission Article 28 DSA guidelines[71]

Aim: Help online platforms to ensure that minors enjoy a high level of privacy, safety and security on their platforms, and help Digital Services Coordinators (DSC) when they apply and interpret the article. Guidelines are a 'significant and meaningful benchmark on which the Commission will base itself (…) when determining the compliance of providers of online platforms accessible to minors with that provision'.

But, adopting and implementing the measures set out in the guidelines, either partially or in full will not automatically entail compliance with Article 28 (1): only the CJEU can give authoritative interpretation of EU law.

Four general principles underpin the guidelines:

1. Proportionality and appropriateness: online platforms do not all carry identical risks for minors; size, reach and type of service as well as its nature, intended and current use, specific features and user base all need to be taken into account.

[67] Commission press release 28 June 2025, available at https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-online-marketplaces-temu-and-shein-compliance-digital-services-act.
[68] Commission press release 18 June 2025, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1551.
[69] Commission Decision of 5 August 2024 relating to a proceeding under Article 71 of Regulation 2022/2065, C(2024) 5654 final.
[70] Commission press realease of 16 May 2024, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664.
[71] Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065.

2. The protection of children's rights: the United Nations Convention on the Rights of the Child and Articles 24 and 21 of the EU Charter on Fundamental Rights need to be taken into account.

3. Privacy, safety and security by design: these elements should be integrated by default in the design, development and operation of their services.

4. Age-appropriate design: services should be designed in alignment with the development, cognitive and emotional needs of minors.

Online platforms need to undertake risk reviews to decide on the correct measures to protect minors at least on an annual basis or whenever they make a significant change to the design of the platform. These risk reviews should also be made available to their DSCs.

Service design features: age assurance (age verification and age estimation); registration; default account settings; removing some settings, features and functionalities; online interface design and other tools, including on the use of AI features; recommender systems and search features which should in particular be tested and adapted and allow minors to control them; and enhanced content moderation policies and practices.

Protection against economically exploitative practices: advertising, product placements, the use of in-app currencies, influencer marketing, sponsorship or AI-enhanced nudging are listed as examples of persuasive commercial practices against which minors should be protected.

Reporting, user support and tools for guardians: special child friendly features should be available (including anonymity). Platforms should make available tools for guardians to help them manage the protection of minors. They should be easy to use, without having to create an account, they should apply regardless of the device/operating system, and minors should be notified that they have been activated.

Governance: this includes for instance the development of internal policies, dedicated persons or teams within the platform, fostering a culture of protection of minors and of child participation, awareness raising of children's rights

3.3 Unlevel Playing Field and Internal Market Fragmentation

To the extent that they are not intermediary services, some online services (e-commerce websites, video gaming platforms, gambling websites, porn services, AI agents, etc) do not fall under sector-specific rules and are only covered by horizontal rules. As shown above, there are only very few horizontal rules at the EU level that protect minors online and they only address specific aspects.

Other services (online platforms including VSPs and very large online platforms and search engines, providers of linear and non-linear audiovisual services) are subject to more rules to protect minors online and are under the supervision of oversight authorities. It seems obvious that this unlevel playing

field is detrimental to the protection of minors. This also undermines the principle of technological neutrality.[72] Filling the gap is a laudable ambition in the spirit of making sure that all online actors protect minors online.

We are also witnessing that some Member States are concerned that there are not enough rules to protect minors online and are adopting national laws such as in France[73], Spain[74] and Italy[75], which place more obligations on online platforms and 'information society services' in general. As the Commission has repeatedly said in the context of the Regulatory Transparency Procedure[76], these national rules are most often not in line with the country-of-origin principle of the E-commerce Directive or with the full harmonisation approach of the DSA[77].

This implies that to the extent possible, more rules should probably be adopted at the EU level and not at the Member State level.

3.4 How Could the DFA Address the Lack of EU Rules to Protect Minors Online?

In a recent resolution[78], the European Parliament called on the European Commission to further improve the Commission's non-binding guidelines on Article 28 DSA and that further legislative action might be required. It calls for a rapid enforcement of the rules both at the EU and national levels, while also asking the Commission to strengthen the protection of minors online in the upcoming DFA.

It calls on the Commission to propose "legislation that mandates age-appropriate design, and safety by design and by default requesting that all platforms and other traders include the necessary risk-based safeguards in their recommender systems, ban engagement-based recommender algorithms for minors, ban the most harmful addictive practices and disable other addictive design features by default for minors, where appropriate."

The European Parliament also proposes that an EU-wide digital majority age of 16 is introduced to access social media (and certain VSPs and AI companions). This demand echoes the demand of the Council, that also stresses the importance of protecting minors, including through a digital age of majority for accessing social media, while respecting national competences.[79] Age assurance is also a

[72] CERRE Issue Paper, The AI Act and Technological Neutrality, Zach Meyers, Daniel Schnurr , Pierre Larouche, November 2025, https://cerre.eu/wp-content/uploads/2025/11/AI-Act-Implementation-Forum-2025_-AI-Act-and-Tech-Neutrality_FINAL.pdf

[73] For instance, Law of 21 May 2024 to secure and regulate the digital space ("Loi Sren"), Arcom decision of 9 Oct. 2024 on binding standards for online age verification systems, Law of 7 July 2023 to establish a digital majority and to combat online hatred, art. 4, not applied in practice as European Commission sent a reasoned opinion to France under the EU Regulatory Transparency Procedure.

[74] A draft "Organic Law for the Protection of Minors in Digital Environments".

[75] For instance, age verification for porn websites (Law 159 of 13 Nov. 2023 converting into law a Law decree on the security of minors of 15 Sep. 2023) ; rating and access control measures for harmful video games and online videos (AGCOM regulation of July 2019 and guidelines that implement art. 10 of legislative decree 203 of Dec. 2017 amending art. 33 of the 2016 Cinema Law): Parental control for Internet service providers (Article 7bis of Law 70 of 25 June 2020 and AGCOM guidelines (9/23/CONS)).

[76] The (EU) 2015/1535 regulatory transparency procedure was set up by Directive 83/189/EEC of March 1983 and was codified in June 1998 (to extend its application to information society services) and in September 2015. The database of notified drafts and responses by the Commission is available at https://technical-regulation-information-system.ec.europa.eu/en/home.

[77] Article 3 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[78] European Parliament resolution of 26 November 2025 on the protection of children online, adopted on 26 November 2025, available at https://www.europarl.europa.eu/doceo/document/TA-10-2025-0299_EN.pdf.

[79] Council Conclusions of 23 October 2025, available at : https://www.consilium.europa.eu/media/d2nhnqso/20251023-european-council-conclusions-en.pdf.

key topic since, to the extent that special rules are introduced to protect minors online, online traders and platforms need to be aware that users are minors.

The question is therefore to what extent the DFA will be able to address all these demands, including that of age assurance.

As highlighted above, it is becoming increasingly clear that the DFA will have a special focus on the protection of minors. Although this is laudable, it does also pose a challenge for the architecture of EU consumer law and could complexify the regulatory situation.

Despite this theoretical issue, the DFA could certainly provide some level of protection for minors in their relationship with all online traders.

In particular, the DFA could build on the current approach of the UCPD, which considers that minors can be vulnerable consumers and could extend this to consumer protection law more generally.

To address the level unlevel playing field directly; the DFA could introduce a general ban – similar to the one in **Article 28 (2) DSA** according to which online traders **should not present advertisements based on profiling (as defined in the GDPR) by using the personal data of minors** (to the extent that they are aware, with reasonable certainty, that they are minors).

To the extent that the DFA does introduce special rules for minors, the question of age assurance will arise. The approach taken in the Article 28 DSA guidance seems sensible to delineate when age estimation[80] or age verification[81] technologies should be used. In the absence of EU-wide rules on age assurance at the moment, the DFA could refer back to these Commission guidelines and to the EU-wide age verification solution (app), pending the entry into force of EU Digital Identity Wallets, which will be able to trigger tokens to provide evidence of age. The Commission is also working on guidance under the DSA on age estimation technologies.

The DFA could introduce a general ban – similar to the one in **Article 28 (2) DSA** according to which online traders **should not present advertisements based on profiling (as defined in the GDPR) by using the personal data of minors** (to the extent that they are aware, with reasonable certainty, that they are minors).

We argue that given the current state of the debate, the DFA should not seek to address the fundamental societal question of a potential social media ban for minors.

[80] These allow a provider to establish that a user is likely to be of a certain age, to fall within a certain age range, ot to be over or under a certain age.
[81] This consists of systems that rely on physical identifiers or verified sources of identification that provide a high degree of certainty in determining the age of a user.

3.5 The DFA Needs to Take into Account the Interplay of Rules

In any event, the DFA will need to take into account the interplay between any new requirements it introduces on the protection of minors and other EU sector-specific rules on the protection of minors. An added important element to bear in mind is the enforcement of the rules.

The interplay between the existing rules is not straightforward, although some aspects are relatively clear because they have been addressed in Commission guidance (which has not been reversed by the CJEU).

Although non-binding, the Commission's guidance on the UCPD states that in relation to the AVMSD (i.e., linear and non-linear audiovisual services and VSPs), the UCPD applies to unfair commercial practices occurring in audiovisual media services, such as misleading and aggressive practices, to the extent that they are not covered by the provisions of the AVMSD itself.

The question of the interplay between the GDPR and the sector-specific rules of the AVMSD and the DSA will most probably be settled similarly. Both legislations have introduced special rules, and these will need to be complied with by the services in the scope of these legal instruments.

The more difficult area is that of the interplay between the rules of the DSA and those of the AVMSD for VSPs. VSPs need to comply with both sets of obligations, and also with the national rules derived from the transposition of the AVMSD in their country of establishment.

The European Commission's recently published study to assess the interplay of the DSA with other pieces of EU legislation and the recommendations from this study has acknowledged some difficulties already.[82] The report notes for instance that the rules on the protection of minors of the AVMSD and the DSA share the same protective objective but that their application is inconsistent:

> *« For example, a platform that is both an online platform under the DSA and a video-sharing platform under the AVMSD must simultaneously comply with the general duty to safeguard minors and with the sector-specific rules governing audiovisual content. For VLOPs, this layering is further compounded by the systemic risk assessment and obligations in Articles 34 and 35 DSA, which include risks to children's rights. The result is not a direct contradiction but a fragmented regime, with overlapping standards and authorities »*

Although enforcement is not the focus of this report, it is important to note that the public enforcement of the rules on the protection of minors regarding the sector-specific rules follows distinct paths. For instance, the rules derived from the DSA are enforced by the national competent authorities (DSCs) and/or by the European Commission for very large online platforms/search engines. Regarding VSPs, and linear and non-linear audiovisual services, the media regulatory authorities are

[82] Commission report and Commission Staff Working Document from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Article 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts {SWD(2025) 368 final.

in charge. The enforcement of consumer protection legislation is mostly done by national courts, and sometimes by national administrative bodies/authorities.

The Commission should therefore be mindful in its upcoming DFA to address the question of how to make sure that rules deriving from multiple pieces of EU legislation on the protection of minors are enforced coherently. The guiding principle should be that the public enforcement of the rules should be as clear and simple as possible, and avoid any form of duplication. The AVMSD is also under review, and a proposal to review the directive is expected to be adopted in the third quarter of 2026. Work on the review of the directive should acknowledge the adoption of the DSA and of the Article 28 guidelines in an effort to reduce these overlapping standards.

4. Addictive Design

Concerns about addictive design in the digital sphere were brought firmly into the EU policy debate by the European Parliament's 2023 resolution on "Addictive Design of Online Services".[83] This resolution called on the Commission to examine potential policy initiatives to address its finding that *"digital addiction and persuasive technologies are problems that require a comprehensive regulatory response from the EU, with a series of supportive policy initiatives, to meaningfully address digital addiction and empower citizens with the ability to determine how they use digital services and products to further their own goals and be protected against new forms of addiction and problematic uses of the internet".* (EP resolution, Para 2)

The resolution also urges the Commission *"to foster ethical design of online services by default"* (Para 11), including *"a digital 'right not to be disturbed' to empower consumers by turning all attention-seeking features off by design and allowing users to choose to activate these features by simple and easily accessible means, possibly with an attached mandatory warning of the potential dangers of activating these opt-in features, offering consumers real choice and autonomy without burdening them with an information overload."* (EP resolution, Para 10)

The Commission is proposing to address these concerns through the forthcoming DFA. In this section, we first consider the rationale for regulation in this area, including what is meant by addictive design, why it matters, and the extent to which existing regulation addresses the identified concerns. We then discuss the Commission's possible policy measures relating both to general addictive design, including more specifically video gaming design.

4.1 The Rationale for Regulation in this Area

4.1.1 Concerns About Addictive Behaviour

There is growing evidence that individuals' online activity and video gaming activity can be both excessive and problematic, and that there may be societal and consumer protection concerns arising as a result.[84] These concerns are primarily non-economic, relating to individuals' mental health and their more general mental development, for example, related to weakened educational motivation and achievement, or degraded social interaction. Even physical fitness can potentially be harmed.[85] However, they can also be economic, for example, individuals may spend excessively, and excessive engagement can potentially be monetised by providers through advertising revenues even if the users themselves pay nothing.

Young people appear especially likely to be vulnerable, and are also the most likely to suffer long-term effects, given that they are still developing. Such harmful effects are also likely to have the greatest long-erm effects of European competitiveness, if they fail to develop much needed skills or exhibit

[83] P9_TA(2023)0459 – Addictive design of online services and consumer protection in the EU single market – European Parliament resolution of 12 December 2023. https://eur-lex.europa.eu/eli/C/2024/4164/oj/eng.

[84] For example, see Lopez-Fernandez, O. and Kuss, D., Harmful Internet Use Part I: Internet addiction and problematic use, EPRS, STOA, p. 51, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624249/EPRS_STU(2019)624249_EN.pdf.

[85] For example, Kokko, S., Martin, L., Geidne, S. et al. *Health behaviours associated with video gaming in adolescent men: a cross-sectional population-based MOPO study*. BMC Public Health 20, 415 (2020). https://doi.org/10.1186/s12889-020-08522-x.

long-term mental health issues. However, concerns about addictive behaviour are not exclusive to young people, and certainly not exclusive to minors.

Such "addictive behaviour", sometimes referred to as "dopamine scrolling"[86], does not necessarily imply that the individuals concerned exhibit a formal "addiction" disorder. To assess whether a behaviour should be recognised as a formal addiction disorder, major health bodies such as the WHO typically consider the extent to which traditional addiction symptoms such as preoccupation, giving up other activities, withdrawal difficulties, continuing despite problems, deceiving/covering up, adverse moods, risking/losing relationships/opportunities. That is, it would take more than evidence of people simply spending more time or money online than they intend, and regretting doing so, for this to be classed as an addictive disorder.

In practice, 'gaming disorder' has been formally recognised by various health bodies. 'Digital addiction' has not, although there is evidence of social media having neurophysiological effects that are very close to addiction.[87] Nonetheless, "addictive behaviour" remains of concern in both contexts, even if this does not imply a formal "addiction" disorder.

It is also important to note that many individuals exhibit self-control issues, in that they engage in certain online activities, such as social media and video gaming, more than they intend to, and then regret doing so, even if this doesn't qualify as 'addictive behaviour'. For example, Allcott et al (2022) find that self-control issues underpin 31% of social media use, [88] even if only a small proportion of users are likely to exhibit a formal disorder.[89]

4.1.2 Concerns About Addictive Design

The focus of the European Parliament resolution, and ensuing Commission work on the DFA, is "addictive design" features of the user interface (or "choice architecture") facing users that can drive such excessive and problematic use of digital devices and video gaming.

We know from behavioural science that the choice architecture facing individuals can have strong effects on their behaviour. Developers have an incentive to introduce design elements intended to enhance engagement as they can monetise that engagement, for example, through sales of advertising or in-game purchases. They may not intend to do harm, and indeed, such engagement-building design elements may not harm those who use the services responsibly. Nonetheless, there is a risk that they can lead to addictive behaviour on the part of vulnerable individuals.

Specific negative design elements highlighted by the European Parliament resolution as raising concerns on digital devices include: 'infinite scroll', 'pull-to-refresh', 'auto-play', personalised recommendations, 'recapture' notifications, and other elements that encourage engagement like the 'like-button', 'read-receipt functions', '[…] is typing' and ephemeral content. (EP resolution, Para L).

[86] Sharpe BT, Spooner RA. *Dopamine-scrolling: a modern public health challenge requiring urgent attention*. Perspect Public Health. 2025 Jul;145(4):190-191. https://pmc.ncbi.nlm.nih.gov/articles/PMC12322333/#bibr7-17579139251331914.
[87] Satani A, Satani KK, Barodia P, Joshi H. *Modern Day High: The Neurocognitive Impact of Social Media Usage*. Cureus. 2025 Jul 8;17(7):e87496. Doi: 10.7759/cureus.87496.
[88] See Allcott, H., Gentzkow, M., & Song, L. (2022). Digital Addiction. *American Economic Review, 112*(7), 2424-2463. https://doi.org/10.1257/aer.20210867 and Hoong, C.Y. (2021). Self control and smartphone use: An experimental study of soft commitment devices. *European Economic Review, 140*, 103944.
[89] See World Health Organization, https://www.who.int/news-room/questions-and-answers/item/addictive-behaviours-gaming-disorder.

There is a reasonably strong evidence base on the addictive nature of several of these design features, which is too extensive to summarise effectively here. This evidence highlights various underlying mechanisms for these effects, from simply removing friction to continuing engagement, to triggering dopamine release through variable reinforcement, to creating persistent habits that continue even when users actively wish to reduce use, to triggering feelings of FOMO (fear of missing out).

Moreover, features can exacerbate individuals' self-control issues, even if this falls far short of comprising 'addictive behaviour. For example, the European Commission's Digital Fairness Fitness Check identified, through a consumer survey, that "31% of consumers reported spending more time or money than they intended because of specific features such as the autoplay of videos, receiving rewards for continuous use or being penalised for inactivity."[90]

4.1.3 Benefits of 'addictive design' features

At the same time, many people engage in online activity and video gaming on a healthy and responsible basis, and indeed it provides benefits, for example in terms of useful relaxation, social connection and skills development. As such, and in contrast with some other jurisdictions where certain services have been banned for certain age groups[91], the EU is not proposing any access bans at this point in time.

Moreover, the so-called 'addictive design' features listed by the European Parliament can also have positive benefits.

- Even to the extent that their main effect is to enhance engagement, these features can increase engagement and habit-formation in relation to beneficial behaviours, for example by fostering skills development (video gaming) and self-expression (social media). Even completely mindless breaks can be mentally restorative.[92]
- In addition, certain of these features have benefits that are unrelated to any effect on engagement. For example, many people value read receipts; the use of ephemeral content allows for more spontaneous, authentic and light-hearted exchanges without creating anxiety about how these might be perceived long-term; if a video-sharing app is being used responsibly for relaxation purposes, then autoplay will tend to enhance the relaxation process and can aid the discovery of interesting new content (and indeed, autoplay of videos on YouTube is arguably not inherently any different to watching a linear TV channel.)

Recommendation 4.1: Given the positive aspects of potentially addictive design features, any regulation needs to be carefully designed, if the positive aspects of these features are not to be lost

[90] Commission Staff Working Document Fitness Check on EU consumer law on digital fairness (aka Digital Fairness Fitness Check), 4 Oct 2024, Section VI.1.2. https ://commission.europa.eu/document/707d7404-78e5-4aef-acfa-82b4cf639f55_en.

[91] For example, as of December 2024, *Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024* banned under-16s from social media, with no exceptions for parental consent. See https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer.

[92] Atsunori Ariga, Alejandro Lleras, Brief and rare mental "breaks" keep you focused: Deactivation and reactivation of task goals 35re-empt vigilance decrements, Cognition, Volume 118, Issue 3, 2011, Pages 439-443. https://www.sciencedirect.com/science/article/pii/S0010027710002994.

for those that engage responsibly online. In addition, overly intrusive regulation could risk pushing vulnerable users towards deliberate circumvention or even into less safe unregulated spaces.[93]

4.1.4 Is there a Regulatory Gap?

As has already been highlighted in the section on protection of minors, there are a number of pieces of EU legislation that are potentially relevant to digital addiction issues. However, as described briefly in this section, none of these provide a complete horizontal legal framework, nor do they provide the sorts of enhanced controls for device users that are envisaged under the DFA.

Consumer Protection Law

UCPD provisions can be interpreted to restrict some types of addictive design. For example, the CPC Network is currently taking action against Temu under UCPD, including in relation to "forced gamification" whereby consumers are forced to "spin the fortune wheel" to access the marketplace.[94] This design aspect risks going beyond simply driving user engagement to foster addictive behaviour. In March 2024, the Italian consumer authority also fined TikTok for UCPD breaches that relate to addictive design features, determining that they were aggressive sales practices under Article 8 UCPD.[95]

For video gaming, we also note that the CPC's 'Key Principles on in-game virtual currencies' are based on its interpretation of UCPD, CRD and UCTD.[96] For example, many video gaming apps charge for in-app digital content or services on the basis of virtual currencies, which can lead to excessive spending and game use.[97] Based on Article 6(1)d) and Article 7 UCPD, the CPC's Principle 1 proposes that price indications should be clear and transparent, and that this includes requiring that real-world money prices are shown alongside virtual currency prices for in-game purchases.

The CPC's principles are all relevant to addictive design, but Principle 7 is of particular interest. Based purely on UCPD, this states that *"Game design and gameplay should be respectful of different consumer vulnerabilities"*, and includes a requirement that game developers should *"avoid basing the business model on practices exploiting vulnerable consumer's willing to spend excessive amount of real-world money in a video game."*

However, while the CPC's Temu investigation and Principles for in-game currencies show that consumer protection law can go some way towards addressing addictive design issues, the CPC's interpretation of the law is untested in Court and subject to ongoing constructive dialogue with the sector. For example, some video gaming providers consider that the CPC's Principle 1 goes too far and

[93] For example, in 2019 China introduced a law to limit video gaming for under 18-year-olds to 90 minutes per day on weekdays and three hours on weekends, with no gameplay from 10pm to 8am. A survey has since found that 77% of minors are getting around this by using other people's identities to register for the games (typically their parents'). https://global.chinadaily.com.cn/a/202408/20/WS66c3e9a1a31060630b923e74.html. Meanwhile, there have been examples of minors being scammed by services promising curfew workarounds. https://www.sixthtone.com/news/1009330.

[94] European Commission Press Release, *Commission and national authorities urge Temu to respect EU consumer protection laws*, November 2024, https://ec.europa.eu/commission/presscorner/detail/fi/ip_24_5707.

[95] Italian Consumer Authority, 14 March 2024, https://www.agcm.it/media/comunicati-stampa/2024/3/PS12543-.

[96] The Consumer Protection Cooperation Network's Key Principles on In-game Virtual Currencies, Mar 2025. https ://commission.europa.eu/document/8af13e88-6540-436c-b137-9853e7fe866a_en.

[97] https://storage02.forbrukerradet.no/media/2024/08/get-played-240523-2.pdf.

that consumer protection law only requires that the price of virtual currency (in real world currency terms) be provided at the time of purchasing the virtual currency.[98]

As such, even where there is an overlap with consumer protection law, DFA provisions could usefully provide greater legal clarity and certainty. Moreover, as is discussed further below, it seems highly unlikely that consumer protection law could be employed to achieve everything the Commission is hoping to cover in this area under the DFA.

Digital Services Act (DSA)

The DSA is also applicable to some forms of addictive design, specifically:

- Art 25 DSA: prohibits use of interfaces that impair or hinder users' ability to make free and informed decisions;
- Art 27 DSA: requires transparency about recommender systems (which arguably include the algorithms that curate social media feeds), including enabling control options;
- Art 28: requires heightened protection for minors for online platforms (not just VLOPs). Platforms must implement "appropriate and proportionate measures" to ensure a high level of privacy, safety and security of minors;
- Art 34/35 DSA places additional requirements on VLOPS to identify and mitigate risks, both in relation to a high-level of consumer protection (Art 34(1)(b)) and specifically in relation to minors and serious negative consequences to the person's physical and mental well-being (Art 34(1)(d)).

There is also clear potential to use these combined measures to address addictive design on the part of platforms targeted at minors. Indeed, the Commission has published Article 28 Guidelines that address several addictive design elements that are intended to be included within the DFA, albeit only for minors. For example:

- It recommends that the following be set as off by default for all minors: default autoplay; push notifications; features that may contribute to excessive use, such as the number of likes, reactions, streaks, the "… is typing" function, and read receipts; and recommendations of other accounts (Para 57(b));
- It recommends that minors should not be encouraged or enticed to change these defaults, should be able to do so on a temporary time-limited basis, and should be able to return to all default settings with a one-click reset (Paras 57(c)–58(b));
- It recommends that certain design features should be switched off completely for minors, including infinite scrolling, artificial notifications, signs communicating scarcity or urgency, and the use of virtual rewards for performing actions on the platform (Para 61(b)); and
- It recommends that the platform should provide customisable, visible, easy-to-access and use, child-friendly and effective time management tools, and use of active notifications to inform minors of the time spent online (Para 61(c)).

[98] The PEGI Code of Conduct (discussed further below) includes additional provision on price transparency (Article 8), https://pegi.info/pegi-code-of-conduct.

Further, platforms designated as VLOPs are required to mitigate any risk that addictive design leads to a systemic risk of serious negative consequences to physical or mental well-being, and not just for minors. The European Commission is already enforcing in this area and has preliminarily found TikTok to be breaching the DSA for failing to adequately assess and mitigate risks to minors and vulnerable adults arising from addictive design features such as infinite scroll, autoplay, push notifications, and its highly personalised recommender system.[99] It has also (as mentioned in Section 3) has separately accepted commitments from TikTok to suspend its 'task and reward' programme in the EU, given the risk of it having addictive effects.[100] It too is investigating Temu, in parallel with the CPC investigation under UCPD, including in relation to its "Spin the fortune" wheel.[101] Finally, it is investigating Meta (Facebook and Instagram) in relation to the risk that its online interfaces cause addictive behaviour, albeit only in respect of minors.[102]

This DSA provision can be used to require VLOPs not only to suppress harmful addictive design and also to introduce enhanced controls of the sort under consideration for the DFA. However, there remains a regulatory gap.

- First, and most critically, many relevant parties – including both app developers and video gaming platforms – are either not in scope of the DSA or are not designated as VLOPs under the DSA. Indeed, many app developers may not be constitute intermediaries and thus may not fall under the DSA at all. Services that use VLOPS to access consumers may be indirectly covered, given they contribute to the risk associated with the VLOP, but this is not currently clear and VLOPS are understandably reluctant to act as enforcement authorities over their business users.
- Second, although all digital intermediaries are subject to Article 28 DSA, it is not just minors that exhibit excessive and problematic use, even if the concerns may be highest for them.
- Third, the Article 28 DSA Guidelines are not legally binding, and if tested through litigation, the Courts could view them as going beyond what the law in fact requires.
- Fourth, although Article 25 DSA is not restricted to minors, it could allow for potential prohibition of addictive design features, whereas what may be more valuable – as discussed further below – is a requirement to provide users with enhanced tools to control certain design features and to control their own online and video gaming activity. It is hard to see how this could be achieved through Article 25 DSA. (Article 27 DSA does incorporate the potential for enhanced controls, but these relate only to recommender systems).
- Fifth, it is possible that some enhanced controls would be more effectively provided at the device or video gaming platform level (in settings) rather than within individual apps/games. As will be discussed later, there are pros and cons of such centralisation, but it is in any case

[99] European Commission Press Release, *Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act,* 6 Feb 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_312.

[100] European Commission Press Release, *Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward programme in the EU*, 22 April 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227.

101 European Commission Press Release, *Commission opens formal proceedings against Temu under the Digital Services Act*, 31 October 2024.

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5622

[102] European Commission Press Release, *Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram,* 16 May 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664.

not clear that the DSA could be used to require it. Apple's iOS and Google's Android OS are not platforms under the DSA (even though the Apple App Store and Google Play Store are) and none of the video gaming platforms are currently designated as VLOPs.

Audiovisual Media Services Directive (AVMSD)

The AVMSD is also potentially relevant to the question of addictive design in relation to video-sharing platforms, albeit again only for minors. Article 28(1) requires Member States to ensure that video-sharing platform providers take "appropriate measures" to protect: minors from content which may impair their physical, mental or moral development, with "parental controls" given as an example of an "appropriate measure". In principle, this could potentially be interpreted as covering design features such as activity management tools and the ability to switch off design features that promote excessive use. However, it is not clear that such an interpretation would be upheld by the Courts, and in any case, these requirements only relate to video-sharing platforms and to minors.

AI Act

Finally, Article 5(1)(a) of the AI Act prohibits the use of an AI system that deploys purposefully manipulative techniques that materially and harmfully distort people's decision-making behaviour. Article 5(1)(b) extends this to include AI that exploits certain specific vulnerabilities, including age, to materially and harmfully distort behaviour. Under the AI Act, harm can include non-economic harm, such as psychological or physical harm. In principle, this may cover certain addictive design features.[103] However, this only covers AI-driven addictive design, and the interpretation and enforceability of this law is not yet fully clear. As such, this does not fill the regulatory gap identified above.

GDPR (and DMA requirements relating to data consent)

Where addictive design involves personalisation, for example, of feeds on say YouTube or social media, data regulation is also relevant.

Within GDPR, the most distinctive provision for minors is Article 8, which requires that children under 16 need parental consent to use online services that process their personal data, although Member States can lower this to 13 and most EU countries have set it at 13-14. The combination of Article 22 and Recital 71 of the GDPR also implies that data should not be used for profiling or automated decisions for a child (albeit no definition is provided of the term 'child'). The DMA Article 5(2) consent requirements relating to the combination and cross-use of data, imposed on designated platforms, are also relevant here, for adults as well as minors. They have apparently already had the effect of reducing personalisation of feeds.

However, these provisions only address personalised addictive design, and then only in relation to children and DMA-designated platforms.

[103] For example, the Commission has recently released guidelines on the AI Act, and these include the following examples of AI that is likely to be prohibited:
- Under Article 5(1)(a): *"[A]n AI companionship application designed to emulate human speech patterns, behaviours and emotions uses anthropomorphic features and emotional cues to influence users' feelings, dispositions, and opinions, making those users emotionally dependent on the service, incentivising addiction-like behaviour"* (Para 88).
- Under Article 5(1)(b): *"A game uses AI to analyse children's individual behaviour and preferences on the basis of which it creates personalised and unpredictable rewards through addictive reinforcement schedules and dopamine-like loops to encourage excessive play and compulsive usage"* (Para 105).

Self-regulation

Alongside statutory requirements, there is the potential for self-regulation to address residual concerns. For example, PEGI (the Pan European Game Information system) has introduced a Code of Practice for its members which requires: upfront age labelling for games; upfront clarity about in-game purchases; receipts for purchases made with real money; games that allow purchase of in-game currency must show the real-world monetary cost at the point of purchase; paid random items (loot boxes) should be optional and the probabilities transparent and equivalent for all players'; and prohibition of use of in-game items for 'skin-gambling' (deposit for gambling or betting).[104] The video gaming industry has also developed, over the years, many resources and parental guides that are easily accessible and designed to help parents on how to engage with their kids on healthy game play.[105]

Such self-regulation can play a valuable part in changing conduct across a sector, but tends to lack enforcement teeth.

4.2 Designing proportionate, effective regulation

The previous section identified the problem, and confirmed the regulatory gap, but also emphasised the need to ensure that any regulation in this area is proportionate and effective, given the positive benefits many users derive from responsible online activity and video gaming, and even from potentially addictive design features.

In this section, we first describe general principles for policy intervention in this area. We then consider some policy options, before discussing how the Commission's existing list of "possible policy measures" fits with these options.

4.2.1 General Principles for Policy Intervention

As briefly outlined in the section on horizontal issues, smart digital legislation should be based on three general principles: (i) risk-based regulation; (ii) design-based regulation; and (iii) ecosystem regulation. This section briefly explains how these principles can be applied in the subscription economy.

Risk-Based Regulation

First, the regulation of addictive design should reflect the level and balance of risks. Relevant risks include both the risk of harm and the risk of unduly limiting firm and consumer behaviour and associated benefits. Importantly, the level and balance of risks associated with any specific addictive design feature is likely to differ:

- **By type of design feature:** for example, intervening against infinite scroll is more likely to address harmful behaviour, and not inhibit positive behaviour, than intervening against read

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

[105] For example, https://pressplaytogether.eu/,which is available not just at EU-level, but also across Member States and in different EU languages. This campaign has support from Better Internet For Kids, a EU Commission initiative.

receipts;

- **By context:** for example, engagement tools such as "streaks" may play a positive role in, say, health and educational apps, even if they have a harmful effect elsewhere.
- **By type of user:** for example, risks of harm are greater for minors than adults, and also vary across age groups, and thus the regulation should consider treating them differently from adults, and potentially also allow for age-appropriate differentiation across minors; and

In addition, it is important that any legislation is future-proof. We know that both the types of addictive design features and the contexts in which they are used are likely to change over time, and any legislation needs to be sufficiently flexible to be able to address the associated risks. For example, in the UK, the Government has just announced proposals to revise the UK Online Safety Act to ensure that they cover AI chatbots as well as social media, and to restrict the use of VPNs by minors (since these can be used to undermine safety regulations).[106] The UK proposals also include a requirement that providers preserve the data of minors in case of death, so that the relevant conduct of the provider can be properly assessed.

Recommendation 4.2: Legislation for addictive design should ensure that it is sufficiently risk-based to enable different design features, users and contexts to be treated differently, including over time.

Design-Based Regulation

Second, while transparency obligations and prohibitions can be valuable in many areas of consumer protection law, there has been an increasing legislative focus in recent years on the choice architecture that consumers face, and in particular on "positive" design rules that prescribe that users should have certain design choices.

In the context of addictive design, such design-based regulation could usefully take the form of **enhanced controls**, which users can employ to empower them to better address their own behavioural tendencies (and those of minors for whom they are responsible). These could include two key types of controls:

- **Activity, spending and notifications controls**, which users can employ to limit their own online activity, maximum spend, and the notifications they receive, ideally on an app/game, app/game category and overall device/platform basis. Such controls have been found to have strong effects when taken up by users.[107]
- **controls relating to specific addictive design features**, enabling users to switch them on or off, or otherwise alter them. These latter controls could also be set as **'safe by default'**.

'Safety by default' is a form of "fairness by design" discussed in Section [1]. It would essentially involve controls being set by default to options that are directly designed to mitigate the risk of addictive

[106] UK Government Press Release, *PM: "No platform gets a free pass": Government takes action to keep children safe online*, 15 February 2026, https://www.gov.uk/government/news/pm-no-platform-gets-a-free-pass-government-takes-action-to-keep-children-safe-online#:~:text=Speaking%20to%20parents%20and%20young,to%20the%20function%20being%20removed.
[107] See Allcott et al (2022), footnote 87.

behaviour. For example, controls for specific addictive design features could be set to off, notifications could be silenced at night, activity controls per app could be set at 15 minutes, etc.

The benefit of setting controls as 'safe by default' is that there is a significant risk that those who would most benefit from such controls will not in fact use them. This could in principle militate towards setting controls as 'safe by default' reasonably widely. However, we also know that users are inclined to stick with defaults, and this approach could lead to controls being set too restrictively for the vast majority of users, who use their devices responsibly. As such, it may be excessive to set all controls as "safe by default" , but we consider there to be particular merit in adopting this approach for minors (with the additional potential provision that parental consent is required to alter the default, or at least that parents are notified).

Recommendation 4.3: Legislation for addictive design should seek to increase the availability and use of enhanced controls. Consideration should also be given to setting controls as 'safe by default', especially for minors.

Ecosystem Regulation

Finally, the regulation of addictive design should take an "ecosystem approach", recognising the role of intermediaries in interactions between suppliers and consumers. In this context, the key issue to be considered is whether certain enhanced controls may be better imposed at system level (that is, on smart mobile OS providers or video gaming platforms), with app and game developers then able to rely on these system-level controls for their compliance in relation to these controls.

There are important pros and cons of such system-level controls. On the negative side, they arguably reduce the extent to which individual services can design controls to reflect the specific level and balance of risk associated with their service. It would also require coverage of apps that were side-loaded, which may not be technically straightforward and could risk undermining the attempts of the DMA to restrict the gatekeeper power of OS providers. On the positive side, such centralised controls may be more effective, with users more likely to be aware of them and experienced in using them. This is important since their effectiveness clearly depends on their being adopted.

Overall, so long as the technical issues can be overcome, system-level controls would seem more suitable for *activity, spending and notifications* controls than for *controls relating to specific addictive design features*. For the former, there are clearly benefits for users of being able to control their activity and spending across multiple apps. For the latter, the overall level and balance of risks are likely to be more heavily dependent on the particular service and context in which they are employed.

We note that such controls are already provided to some extent. For example, Apple and Android smartphones include a range of controls that can be used to limit online activity (overall, by app/game and by app/game category) and the use of notifications (again, by app). They also include extensive parental controls, which enable responsible adults to monitor and control the online activity of minors. These are summarised in Table 2 below.

Table 2 : Activity, spending and notifications controls on Apple iOS and Android OS[108]

	Apple	Android
Information on past activity	Daily and weekly reports showing time spent in apps and on devices.	Dashboard showing time in apps and notifications
Screentime limits	Set daily screentime limits for all apps, app categories (e.g, social) or specific apps. Can be set across devices. If set by parents, can't be changed by children. Parents are notified if they try to do so.	Set daily screentime limits for all apps, app categories (eg social). Parents can set total device screentime limits.
Friction involved in temporarily overriding limits	For adults – very easy For children – they need to ask parent to approve.	For adults – very easy For minors – they need to ask parent to approve.
Spending limits	Parents can require that minors gain parental consent for any purchases. This set to on-by-default for under-13s, when family sharing is used.	Parents can require that minors gain parental consent for any purchases.
Bedtime mode	Limits access to specified apps	For minors – parents can lock the device. Parents can also lock the minor's device remotely at any time.
'Heads Up'		Reminds you to look up while walking
Notifications	Turn notifications off or customise (including requiring grouping of notifications), on a per app basis.	Turn notifications off or customise (including requiring grouping of notifications), on a per app basis.
Focus mode	Stops notifications from specified apps for limited period	Stops notifications from distracting apps for limited period

[108] NB The tools listed in this table are those that relate to controlling activity or notifications. We note that there are many other types of controls too, such as relating to communication safety (which detects nudity in images), ability to speak to strangers (see https://www.apple.com/families/), or (for adults) tools which limit use of a phone while driving.

Likewise, as set out in Table 3, the major video gaming platforms (consoles/stores) frequently offer activity, spending and usage controls, albeit these are typically only for minors, and must be enabled by parents. (Only Roblox, not listed below, appears to enable adults to set their own screentime limits.)

Table 3 : Activity, spending and notifications controls on major video gaming platforms[109]

	XBox	Playstation	Steam	Nintendo Switch
Activity monitoring	Yes (real time and summaries)	Yes (real time and summaries)	Yes (summaries)	Yes (real time and summaries)
Daily/weekly screentime limits	Yes (and per-game limits)	Yes	Yes (and per-game limits)	Yes (but relate to total console use, not per user)
Friction involved in temporarily overriding limits	Parental consent required	Choice of notification only or Parental consent required	Parental consent theoretically required but easy to bypass	None. Notification only
Time of day restrictions	Yes (can set play time window)	Yes (can set play time window)	Yes (can set play time window)	No. Bedtime alarm only
Spending limits	Parental consent for purchases Can set an allowance (funds added to account)	Parental consent for purchases Can set an allowance Monthly spending limit (store only, not in-game)	Parental consent for purchases	No. PIN required but nothing beyond that.

[109] NB As before, the tools listed in this table are those that relate to controlling activity or notifications. We note that there are many other types of content and communications controls too, which relate more generally to child safety.

Despite the controls already in existence, there is clearly substantial variation in functionality. We consider that they could be significantly improved, for both smart mobile devices and video gaming platforms, especially in relation to what is available for adults seeking to control their own usage. This is discussed further below.

Recommendation 4.4: Legislation for addictive design should enable (and possibly require) enhanced *activity, spending and notifications controls* to be set at system-level, which service providers can then rely on for their compliance. ***Controls relating to specific addictive design features* should be set at individual service level.**

It should be noted that the adoption of system-level controls would in no way impose a requirement for the platforms involved to police the DFA compliance of its service users, only that these service users could rely on these system-level compliance for their DFA compliance.

4.2.2 Options for Policy Intervention

In this section, we examine the options for policy intervention in more detail, before turning to compare these options with the Commission's list of "possible policy measures".

Activity, Spending and Notifications Controls

As discussed above, limits on online activity can have a strong effect when people choose to use them. The European Parliament resolution urges the Commission to consider: warnings or automatic locks when users have spent more than a preset amount of time on a specific service; the option for users to restrict access to certain apps between certain times; weekly summaries of total screen time, further broken down by online service; and turning all notifications off by default. (Para 11).

As mentioned above, there are already a number of activity management and notification control tools available to device users, at the device level, to limit the risk of addictive behaviour on smart mobile devices and gaming platforms. However, these are currently viewed as insufficiently restrictive enough to significantly change user behaviour, at least for adults.[110] Activity monitoring alone also appears to have little effect.[111]

Moreover, no such system-level controls are currently provided by video gaming platforms, nor are users on either type of platform currently able to set (daily or monthly) spending limits for themselves.

Recommendation 4.5: The Commission should consider using the DFA to strengthen requirements in relation to these system-level activity, spending and notifications controls.

The most important changes would be:

- First, to require video gaming platforms such as Xbox, Steam, PlayStation and Roblox to

[110] Alberto Monge Roffarello and Luigi De Russis. 2019. *The Race Towards Digital Wellbeing: Issues and Opportunities*. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 386, 1–14. https://doi.org/10.1145/3290605.3300616

[111] Oeldorf-Hirsch, A., & Chen, Y. (2020). *Who Cares about Screen Time? Predicting the use of Mobile Phone Tracking Features*. Paper presented at the ICA Annual Conference 2020, Virtual. Also Saariketo (2019) finds that, while people are initially enthused by monitoring of smartphone use, many are subsequently indifferent. (Saariketo, M. (2019). *Encounters with self-monitoring data on ICT use*. Nordicom Review, 40(s1), 125–140.

introduce tools that allow adult users to control their own activity.

- Second, to enable users to set spending limits by app/game, app/game category, and overall.

Additional possible changes for consideration include the following:

- A requirement that these controls be easy to access, understand and use. (An example might be enabling users to readily alter the default rule for all notifications without having to do this on an app-by-app basis.)[112]

- Increasing the friction involved in temporarily overriding a screen time limit. Currently, this friction is reasonably high for minors (except on Nintendo Switch) but minimal for adults on smart mobile devices.

    - One option for adults, would be to enable adults to identify one or more other adults as 'accountability partners' who have to provide consent to such an override (in much the same way as a parent must do currently). While this service is currently provided by a number of third-party apps, it seems that both the user and any accountability partners need to pay to use the app, which is likely to significantly reduce take-up.

- Revision of the digital content exception under the EU Consumer Rights Directive (Article 16(m)), to allow consumers a short period in which to change their mind when buying digital content such as virtual currency or skins.

- For minors under a specified age (e.g. 16), access to any apps/games could require parents to have set up relevant system-level parental controls, or proactively to have opted out of doing so. (Currently, these are optional for parents, and many parents will likely be unaware of the available functionality).

- For minors under a specified age (e.g. 16?), notifications on smart mobile devices could be required to be off by default.

Controls Relating to Specific Addictive Design Features

The Commission's Digital Fitness Check[113] lists a number of potentially addictive design features that have raised concerns including: autoplay; pull-to-refresh; infinite scroll, ephemeral content; various incentives for continued engagement (e.g., badges, rewards) or, conversely, penalties for disengagement (streaks); push notifications; and gamification of non-gaming environments. In addition, in a video gaming environment, some monetisation features such as loot boxes, pricing of virtual currencies, and 'pay-to-win/progress' models are referred to as potentially addictive design elements.

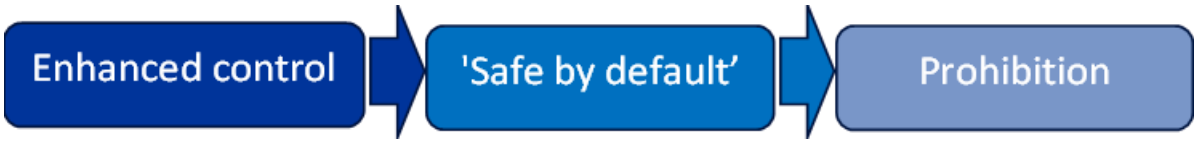
If regulation is to be risk-based, it would be disproportionate to simply **prohibit** all of these specific design features – even if this may be appropriate for some features in some contexts. This is because many of them bring benefits in their own right, or are valuable in fostering positive engagement. Far more proportionate would be for services to give their users (and parents on behalf of minors) **enhanced control** of their own online environment, and the addictive design features that they are

[112] The last of these is currently available on Apple iOS but not on Android OS.
[113] See footnote 86, section VI.1.2.

subject to. This could be complemented by services setting some features as **'safe by default'**, at least for minors.

The following graphic shows these alternative approaches ordered (L->R) from least restrictive to most restrictive. The least restrictive may in fact require more initial system design work, but thereafter are less likely to restrict unduly limit the user's experience of the service.

Figure 1: Approaches to addressing identified features



The effectiveness of these options in limiting the use of harmful addictive design features would also require service providers to consider details such as:

- how easy the controls should be to access, understand and use;
- how easy it is to switch away from the default (e.g. for minors, should it require parental consent?);
- how easy it is to reset to the default; and
- whether it should be possible to temporarily override the restrictions provided as a default, without changing the default, and how big a friction should be involved in doing so.

Moreover, if a system of enhanced controls and defaults in relation to specific addictive design features were to be introduced on a widescale and systematic way, to comply with the DFA, then users should become far more conscious of them and more likely to take the time to understand and use them, further increasing their effectiveness and proportionality.

Thus we consider that:

Recommendation 4.6: The Commission should use the DFA to require the risk-based adoption of enhanced controls and defaults for specific addictive design features (and in extreme cases prohibitions for certain users).

However, we further note the importance of making the DFA future-proof. This militates against including specific rules relating to specific addictive design features in specific contexts, but rather in favour of a more principles-based approach.

Options for principles-based regulation

There are two possible options for achieving such a principles-based approach.

The first would be to **revise UCPD to cover addictive design features**. This would certainly require **clarification of the concept of "transactional decision"** to include all relevant decisions, including those going beyond direct purchasing decisions, such as interacting with content (scrolling, clicking, continuing to use the service). As we note below, this is listed by the Commission as one of its possible

policy measures.[114] However, in addition, UCPD relates to commercial practices which distort consumers' **economic** behaviour. As such, it would likely also require clarification of the concept of **"economic behaviour"** to include any behaviour (attention, continued usage) that can be monetized by the service provider, for example by selling advertising.

However, in our view this approach is not a good option for three reasons. First, refining these concepts in the UCPD may well have **wider consequences** that are currently unforeseen. Second, the UCPD is a **prohibition-based** regulation, and in our view prohibition is unjustified for most of these addictive design features. What is required are enhanced controls and use of defaults, and UCPD isn't a natural vehicle for achieving these. Third, the real concern in relation to these addictive design features relates to their **non-economic effect** on users, not their economic effect. This means that if service providers were to assess their UCPD compliance purely on the economic effects, they may under-comply from the perspective of wider non-economic concerns. Thus:

Recommendation 4.7: Rather than seeking to address specific addictive design features by refining UCPD, it would be more coherent to introduce a new targeted rule within the DFA.

This raises the final question of how such a targeted rule might be designed. The first issue is how to define "addictive design features" when we are concerned to empower individuals to limit their exposure to these features, even if they are not currently exhibiting, or at risk of developing, a formal addiction disorder.

In our view, the guidelines on Article 28 DSA (paragraph 61(b)) provide a useful framework, which avoids any reference to "addiction". This frames the concerns around design features that:

- are persuasive;
- aimed predominantly at engagement; and
- create a risk of harm in the form of extensive use or overuse of the platform or problematic or compulsive behavioural habits.

A key benefit of such a principle-based approach is that it can encompass new design features, that have not yet been identified as being of concern, and may not even yet have been invented.

A second issue is how to frame a new rule. Given that the intention is to require greater empowerment of users, we propose that it should avoid taking a prohibition-based approach (like in UCPD or DSA Article 25) and instead, for online firms providing design features that fit the above criteria:

- to provide controls, and implement default settings, that address the risk of harm;
- to ensure effectiveness though making these controls are easy to access, understand and use, and designing in sufficient friction associated with diverging from the default; and
- to ensure that the risk is specifically addressed for vulnerable users, including minors.

The last of these criteria is important for ensuring that the DFA provides an appropriate complement to Article 28 DSA for non-platform service providers. We consider it appropriate to single out minors

[114] Call for tenders EC-JUST/2024/OP/0001 (internal reference: JUST/2023/PR/JUH1/0096), Topic 2, Measure 1, p. 11. https://ec.europa.eu/newsroom/just/items/820177/en,

here too on the basis that their self-control powers are especially limited and they are more likely to suffer long-term harm from addictive behaviour. Harm to their development and mental health will also have especially serious implications for long-term European competitiveness.

In summary:

Recommendation 4.8: The Commission should consider introducing a targeted rule within DFA for design features that are persuasive, aimed predominantly at engagement, and create a risk of harm in the form of extensive use or overuse of the platform or problematic or compulsive behavioural habits. Firms employing such design features should provide controls, and implement default settings, that address the risk of harm; ensure effectiveness though making these controls are easy to access, understand and use, and designing in sufficient friction associated with diverging from the default; and ensure that the risk is specifically addressed for vulnerable users, including minors.

4.2.3 The Commission's possible policy measures

Having set out our recommendations for regulation, we now consider the Commission's list of "possible policy measures", as set out in the Commission's tender documents for the DFA Impact Assessment work (under Topic 2).[115] It is far from clear how finalised these are, but they nonetheless form a useful basis for discussion here.

For some reason, the Commission separates out what it terms "addictive design" from what it terms "problematic features of digital products", but we address these together below. For clarity (since the Commission duplicates its numbering, we number the former as AD1-4 and the latter as PF1-4. We also do not discuss measure AD1 here, as it is to clarify the concept of "transactional decision' under UCPD, as already discussed in the previous section.

Activity, spending and notifications controls

The Commission lists the following as possible policy measures for **activity, spending or notifications controls**.

> *Measure PF4a - the supplier must clearly offer an in-app or in-game facility to set up limitations on duration of the use, on spending and offer the facility to add 'waiting time' before finalising a purchasing decision; Measure PF4b – integrate dashboards indicating the duration of use and the cumulative amount spent on virtual items. Measures can be cumulated.*

We welcome this option, but would highlight the benefits of requiring that these controls be provided at a system-level, that individual service providers can rely upon for their compliance. We also highlight that we make a number of additional suggestions in this area just below Recommendation 4.5.

Controls relating to "addictive design"

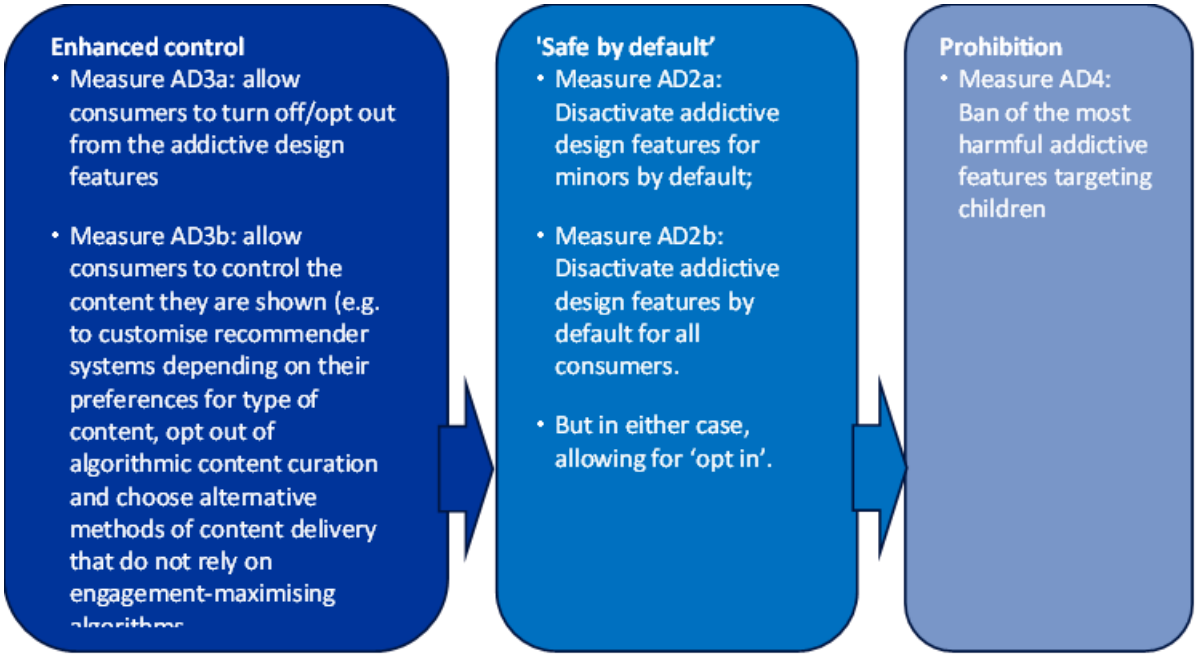
The Commission provides a list of "addictive design features": e.g. notifications, automatic playing of new content; infinite scroll; pull-to-refresh; gamification features (badges, rewards, penalties for

[115] Call for tenders EC-JUST/2024/OP/0001 (internal reference: JUST/2023/PR/JUH1/0096), pp. 11-12. https://ec.europa.eu/newsroom/just/items/820177/en

disengagement etc.); ephemeral content; recommender systems. This list is the same as in the Digital Fitness Check, with the addition of recommender systems.

For these, the Commission then proposes possible measures as set out in Figure 1 below. At this stage, the Commission has not set out which of these options it considers appropriate for which measures. As outlined above, we consider that it would be more appropriate to adopt a principles-based rule in DFA rather than specific rules relating to specific existing design features.

Figure 2: The Commission's possible policy measures for "addictive design" (AD2-4)



Nonetheless, in case the Commission decides to go down an alternative route, we also comment specifically on these options, based on the evidence we have seen. We would support:

- applying Measures AD2a, AD3a and AD3b;
- not applying Measure AD2b (AD3a and AD3b should be enough for adults);
- Not applying Measure AD4 (except possibly to infinite scroll, which does not appear to have strong positive benefits);

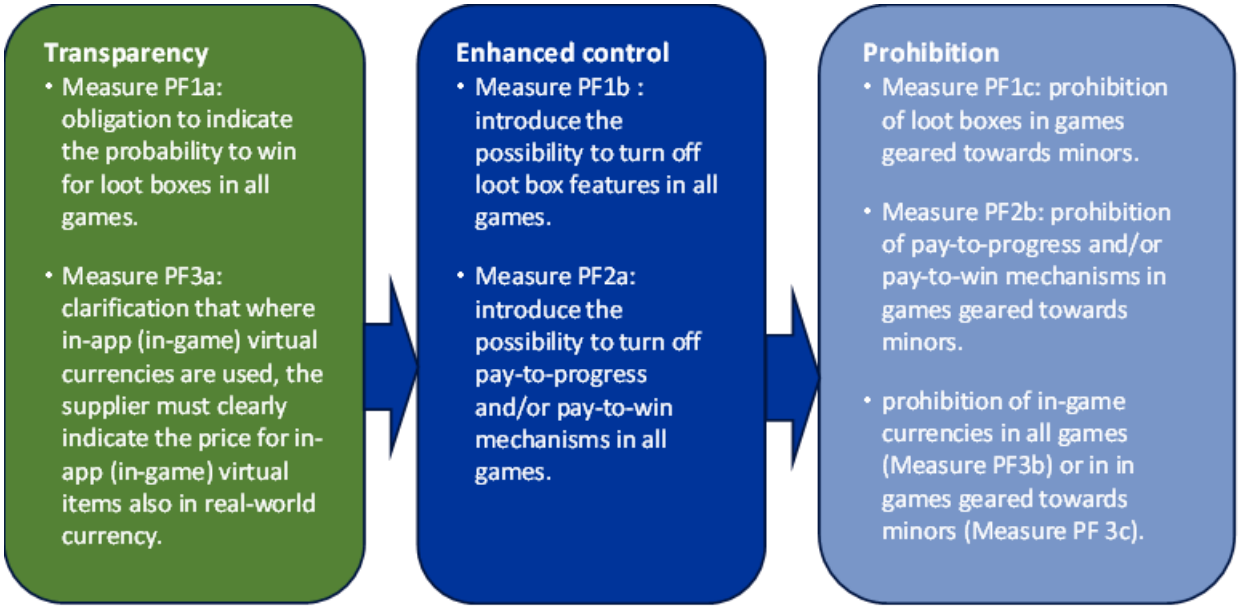
We also note that where minors are treated differently, consideration could usefully be given to differentiating rules by age-band. We would also support the Commission giving consideration to additional rules relating to how easy it is to how easy it should be to switch away from the default, to temporarily over-ride the default, to reset to the default, and how easy these controls should be to access, understand and use.

Proposals relating to "problematic features"

Finally, the Commission also considers separately what it describes as a set of "problematic features of digital products". PF4 was discussed above, and PF1-3 relate to video gaming. The Commission lists

as "problematic features" loot boxes, pay-to-progress/won, pricing in in-game currencies.[116] For these, it only appears to suggest two options: enhanced controls or prohibition, with no 'safe by default' option listed. Additionally, two transparency measures are listed. These are set out in Figure 2 below.

Figure 3: The Commission's possible policy measures for "problematic features" (PF1-3)



Overall, these possible policy measures appear broadly proportionate, with the exceptions of:

- Measure PF1a, since the probability of winning is only one dimension of the addictive potential of loot boxes and arguably unimportant relative to the desirability of "what" you win.
- Measures PF3b and PF3c which seem disproportionate, especially if there is a strengthening of other ways to control the spending of minors (Measure PF4, discussed above).

[116] We note that, relative to the European Parliament resolution, the Commission appears to have dropped its focus on currencies being available only in bundles and skin betting. The removal of the latter may reflect the fact that PEGI has now prohibited this for its members in any case, see footnote 93.

5. Personalisation Practices

5.1 Introduction

Another focus area identified in the Digital Fairness Fitness Check is the use of personalisation practices by businesses. Personalisation techniques are used for ranking recommendations and search results, for advertising, and sometimes for personalised pricing. While personalised advertising, ranking and recommendations are widespread, evidence on the use of personalised pricing is still somewhat inconclusive.

In its final report on the Digital Fairness Fitness Check, the European Commission argues that "EU consumer law cannot be considered sufficiently effective or clear in addressing the multifaceted concerns regarding commercial personalisation".[117] Against this background, the Commission has proposed to address "unfair personalisation practices" in the forthcoming DFA. In this section, we first consider the rationale for regulating personalisation practices, and the extent to which existing regulation addresses the identified concerns. We then discuss the Commission's possible policy measures relating to unfair personalisation practices.

5.2 The rationale for regulation in this area

5.2.1 Concerns regarding personalisation practices

Consumers increasingly encounter personalisation practices on digital markets. The spectrum ranges from targeted advertising via personalised recommendations and search results to personalised pricing. Algorithmic personalisation has a number of positive effects for consumers, for example by making more relevant content available and by reducing search costs. Similarly, from an economic perspective, price discrimination is not harmful per se and can even help to open the market to consumers who might be able to buy a product or service under a uniform pricing system.[118] Therefore, the use of algorithmic personalisation cannot be considered "problematic" as such.

However, there are growing concerns about "unfair personalisation" regarding data privacy, potential exploitation of consumer vulnerabilities, and lack of transparency. In particular, problematic practices include the use of personalisation to exploit users' individual vulnerabilities (e.g. age, emotional or financial distress, mental infirmity) or the use of special categories of personal data (e.g. sensitive data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or health data).

Behavioural price personalisation may also have distributive effects between businesses and consumers as it allows businesses to extract the maximum surplus from consumers. In addition, the opacity of personalised pricing mechanisms could increase consumer search costs.

According to a 2023 consumer survey cited in the Commission's final report on the Digital Fairness Fitness Check 70% of respondents are concerned about how their personal data is used and shared.[119] Moreover, 74% of the consumers believed that their data was misused or unfairly used to personalise

[117] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*. SWD(2024) 230 final, p. 169.
[118] K Heidary, J-P van der Rest and B Custers, Discrimination grounds and personalised pricing: Consumer perceptions of fairness, norm alignment, legality, and trust in markets, 13(4) Internet Policy Review (2024), https://doi.org/10.14763/2024.4.1809.
[119] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*. SWD(2024) 230 final, p. 162.

offers.[120] Additionally, empirical research indicates that many consumers consider first-degree price personalisation that exploits the consumer's individual willingness to pay as unfair.[121]

In brief, while the concerns associated with the misuse of personal data for unfair personalisation practices arguably justify policy intervention, the choice of regulatory tools and the depth of regulation should ensure that consumers do not lose the benefits of personalisation.

5.2.2 Is there a regulatory gap?

The regulations relevant to personalisation practices at EU level are scattered across various legal acts. Generally speaking, EU law sets boundaries to the use and processing of data for the purpose of personalisation practices, stipulates transparency requirements for business that engage in such practices, and prohibits some categories of personalised practices that are considered particularly harmful.

Data protection requirements

As personalisation practices involve the processing of personalised data, they must comply with the fairness and transparency requirements of the GDPR. More specifically, the GDPR sets limits for data collection and transparency requirements for profiling (Art. 22 GDPR).

Consumer protection law

According to Art. 6(1)(ea) CRD traders must inform consumers, where applicable, that the price was personalised on the basis of automated decision-making. Similarly, Art. 13 Consumer Credit Directive requires creditors and credit intermediaries "to inform consumers in a clear and comprehensible manner when they are presented with a personalised offer that is based on automated processing of personal data".[122]

Platform regulation regarding personalisation practices

While EU consumer law only provides for a few transparency requirements regarding personalised pricing and offers, EU platform law contains more far-reaching regulations that specifically concern personalised advertising.

According to Art. 26(3) DSA providers of online platforms must not present advertising to recipients of their service based on profiling (as defined in Art. (4) GDPR) using special categories of personal data (Art. 9(1) GDPR). Additionally, Art. 28(2) DSA stipulates that, providers of online platforms shall not present advertising on their interface based on profiling using personal data of minors. Also relevant in this context is Art. 27 DSA, which imposes transparency requirements on online platforms regarding the main parameters of their recommender systems. If algorithmic recommendations are personalised, the relevant parameters must be specified.

[120] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness*. SWD(2024) 230 final, p. 162.
[121] J Poort and F Zuiderveen Borgesius, Does everyone have a price? Understanding people's attitude towards online and offline price discrimination, 8(1) Internet Policy Review 2019, https://doi.org/10.14763/2019.1.1383
[122] For additional transparency requirements regarding personalised pricing see Art. 10(5)(m) and Art. 11(4)(h) Consumer Credit Directive 2023.

Additional rules apply to Very Large Platforms (VLOPs) and Very Large Search Engines (VLOSEs). Under Arts. 34 and 35 DSA , they are required to conduct risk assessments to identify systemic risks stemming from the design, functioning or use of their service, and to adopt risk mitigation measures in response. In this context, the design of recommender systems and any other relevant algorithmic systems as well as the systems for selecting and presenting advertisements have to be taken into account.[123] More specifically, Art. 38 DSA stipulates an opt-out rule for profiling-based recommender systems.

Additional rules relevant to personalisation practices can be found in the DMA and the AVMSD. Thus, Art. 5(2) DMA sets limits to data combinations by gatekeepers for advertising and Arts. 6a and 28b contain additional rules regarding targeted advertising for minors.

AI Act

Finally, the AI Act prohibits the use of AI systems that involve the deployment of subliminal techniques, purposefully manipulative or deceptive techniques or the exploitation of vulnerabilities related to age, disability or a specific social or economic situation that leads or is likely to lead to significant harm (Art. 5(1) AI Act).

In summary, neither of the legislative acts mentioned above currently provides a complete horizontal legal framework addressing problematic personalisation practices, nor do they provide the sorts of enhanced controls for device users that is envisaged under the DFA.

5.3 The Commission's Possible Policy Measures

Drawing on the three general principles for smart digital regulation outlined above, this section explains how these general principles could be implemented regarding personalisation techniques. We then take a closer look at the Commission's list of "possible policy measures" and analyse how they fit with our general principles.

5.3.1 General Principles for Policy Intervention

As briefly outlined above, smart digital regulation should be based on three general principles: (i) risk-based regulation; (ii) design-based regulation; and (iii) ecosystem regulation.

Risk-Based Regulation

First, the regulation of personalisation practices should be risk-based and differentiate between different practices and use cases according to their specific risk profile. In this perspective, the DFA should address clearly identified harms and ensure that consumers do not lose the benefits of personalisation. In this sense, a risk-based approach first requires an assessment of the various risks associated with personalisation techniques. This necessitates identifying potentially harmful personalisation techniques and weighing up the potential harms and benefits for consumers. For example, the potential harms associated with personalised advertising may be more limited than

[123] See Art. 34(2)(a) and (d) DSA.

those linked to personalised pricing. With a view to the principle of proportionality, different use cases may require a different depth of regulation (opt-out, opt-in, ban).

An example of a particularly harmful personalisation practice is personalised choice architectures or personalised dark patterns. By using personal data, suppliers may create 'persuasion profiles' and create personalised choice architectures which are especially well-designed to achieve harmful effects for specific individuals or groups of individuals. For this reason, there may be merit in imposing relatively strong rules in relation to automated personalised online choice architecture.[124]

Design-Based Regulation

Second, the regulation of personalisation practices should also follow a design-based approach. The aim should be to design user interfaces in such a way that consumers can easily exercise control over personalised features and easily select opt-in or opt-out options. Moreover, it is important that once a user has exercised his right to opt-out, this choice is retained even if the user has closed the app/website and then reopens it again ("persistent choice").[125]

In this regard, it is necessary to clarify what is the appropriate level for voluntary opt-in/opt-out options (e.g., device level, browser, app store, individual application or website level). As the failed cookie regulation shows, regulation at the app/website level may lead to "click fatigue". If possible, device-level or browser-level solutions seem preferable.

Regardless of the level of regulation, the exercise of opt-in/opt-out choices for personalisation should be straightforward for consumers. Related questions are: What is the right level of detail for the design requirements? Should the DFA introduce an easy opt-out/opt-in facility ("privacy button") similar to the recently introduced "withdrawal button" (Art. 11a CRD)? How to ensure technology-neutral design regulation?

5.3.2 The Commission's Possible Policy Measures

Having set out the general principles for regulating algorithmic personalisation, we now consider the Commission's list of "possible policy measures", as set out in the Commission's tender documents for the DFA Impact Assessment work (under Topic 3).[126] It is not yet clear how final these are, but they offer a useful starting point for discussion.

The following table provides an overview of the measures that are currently being considered by the Commission:

Measure 1	Businesses to provide a simple 'opt-out' option at the relevant moment, including at the point where the personalisation is offered, i.e., persistent choice not to receive personalised advertising or offers; of particular interest are the options to realise a meaningful opt out without creating click-fatigue.

[124] C Busch and A Fletcher, Harmful Online Choice Architecture, CERRE Report, May 2024, p. 39.
[125] Bits of Freedom v. Meta, Rechtbank Amsterdam, 2 October 2025, ECLI:NL:RBAMS:2025:7253.
[126] Call for tenders EC-JUST/2024/OP/0001 (internal reference: JUST/2023/PR/JUH1/0096).
https ://ec.europa.eu/newsroom/just/items/820177/en.

Measure 2	Meaningful and easy to manage choice to opt-in to any personalised marketing and offers (non-personalised as default).
Measure 3	Prohibit price personalisation to the detriment of specific groups (children and/or vulnerable consumers) or ban specific practices (e.g., creating or abusing price intransparency).
Measure 4	Prohibit actors that are not online platforms as defined in DSA Article 3(i) presenting advertising based on profiling using the personal data of minors or using special categories of personal data as defined in the GDPR.
Measure 5	Prohibit personalised advertising on the basis of vulnerabilities (extension of AVMSD and DSA prohibitions).

Opt-Out from Personalised Advertising or Offers

Measure 1: Businesses to provide a simple 'opt-out' option at the relevant moment, including at the point where the personalisation is offered, i.e., persistent choice not to receive personalised advertising or offers; of particular interest are the options to realise a meaningful opt-out without creating click-fatigue.

The suggested measure is modelled broadly on Art. 38 DSA which requires providers of very large online platforms and of very large online search engines that use recommender systems to provide at least one option for each of their recommender systems which is not based on profiling (as defined in Art. 4(4) GDPR). The proposed measure aims to extend the personal scope of the opt-out rule to all traders (not just VLOPs and VLOSEs) and to extend the material scope to all personalised advertising and offers (not just recommender systems). Given the broad scope of application of the suggested measure, the choice of an opt-out rule (as opposed to an opt-in or even a total ban) seems appropriate.

For the opt-out option to be effective, the choice must be straightforward for consumers ('without creating click fatigue'). The DFA could follow the example of the DSA in this regard. Art. 38 DSA in conjunction with Art. 27(3) DSA stipulates that, if there are several recommendation options, the function used to select them (including the profiling-free recommendation option) must be "directly and easily accessible from the specific section of the online platform's online interface" where the recommendations are displayed. A simple but effective solution could be a standardised 'privacy button' (modelled on the 'withdrawal button' from Article 11a CRD).

Opt-In to any Personalised Marketing and Offers

Measure 2: Meaningful and easy to manage choice to opt-in to any personalised marketing and offers (non-personalised as default)

Measure 2 goes beyond Measure 1 in that it proposes opt-in rather than opt-out. Non-personalised advertising and offers would thus be the default. Concerning the principle of proportionality, an opt-out rule seems preferable for a general rule on personalised marketing and offers, provided that it is easy for consumers to exercise the opt-out. One possible approach could be combining opt-out and opt-in rules. For example, one could consider introducing an opt-in mechanism for riskier forms of personalised practices (e.g., personalised pricing) and an opt-out rule for less risky cases (e.g., personalised advertising).

Prohibition of Price Personalisation for Specific Groups

Measure 3: Prohibit price personalisation to the detriment of specific groups (children and/or vulnerable consumers) or ban specific practices (e.g., creating or abusing price intransparency)

Measure 3 goes even one step further and proposes a ban on price personalisation. However, the personal scope of the measure is limited to specific groups. The Commission leaves open whether the rule should apply only to minors or also to other 'vulnerable groups'. The latter apparently refers to 'a clearly identifiable group of consumers who are particularly vulnerable […] because of their mental or physical infirmity, age or credulity' (Art. 5(3) UCPD). For reasons of legal certainty, the 'vulnerable group' would have to be clearly defined and also clearly recognisable to the trader. This is likely to be difficult in practice. Therefore, the rule should only apply to minors, if at all.

Even if the scope of application is restricted to minors, the rule must be formulated in such a way that it is predictable for the trader whether the rule applies to a specific case or not. One option would be to formulate the rule along the lines of Art. 28(2) DSA, which prohibits personalised advertising based on the profiling of minors. This rule applies when platform providers are aware with reasonable certainty that the recipient of the service is a minor.

No Advertising Based on Profiling Using the Personal Data of Minors or Special Categories of Data

Measure 4: Prohibit actors that are not online platforms as defined in DSA Article 3(i) from presenting advertising based on profiling using the personal data of minors or using special categories of personal data as defined in the GDPR

Measure 4 aims to apply the prohibitions in Articles 26(3) and 28(2) of the DSA to actors who are not covered by the DSA. This is not only to be welcomed for reasons of consumer protection, but also serves to create a level playing field between platforms and other actors.

This is not only to be welcomed for reasons of consumer protection, but also serves to create a level playing field between platforms and other market actors. However, extending the prohibition in

Article 26(3) DSA would not be sufficient, as the provision does not prohibit 'emotional targeting' or 'emotion-based advertising' (i.e., exploiting insecurity, fear, stress).[127] Measure 5 could close this gap.

Prohibition of Personalised Advertising Based on Vulnerabilities

Measure 5: Prohibit personalised advertising on the basis of vulnerabilities (extension of AVMSD and DSA prohibitions)

Measure 5 concerns a particularly harmful category of personalised advertising that exploits a person's vulnerabilities. The Commission must clarify what is meant by 'vulnerabilities'. This should not only include categories such as 'mental or physical infirmity, age or credulity' (Art. 5(3) UCPD), but also temporary and situational vulnerabilities (e.g., insecurity, fear, stress). The provision should therefore be worded in such a way that it also covers harmful forms of 'emotional targeting' and personalised dark patterns. One challenge will be where to draw the line between permissible persuasive techniques and 'unfair personalisation'.

[127] See K Grisse, in: F Hofmann & B Raue, Digital Services Act, 2025, Article 26, comment 75.

About CERRE

Providing high quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) is a not-for-profit think tank. It promotes robust and consistent regulation in Europe's network, digital industry, and service sectors. CERRE's members are regulatory authorities and companies operating in these sectors, as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach covering a variety of markets, e.g., energy, mobility, sustainability, tech, media, telecom, etc.;
- the widely acknowledged academic credentials and policy experience of its research team and associated staff members;
- its scientific independence and impartiality; and,
- the direct relevance and timeliness of its contributions to the policy and regulatory development process impacting network industry players and the markets for their goods and services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as contribute to the enhancement of those organisations' expertise in addressing regulatory issues of relevance to their activities.

About the Authors

Christoph Busch is Professor of Law and Director of the European Legal Studies Institute at the University of Osnabrück, Germany. He is a Fellow and former Council Member of the European Law Institute (ELI) and an Affiliated Fellow at the Information Society Project at Yale University. His research focuses on consumer law, platform governance and algorithmic regulation.

Amelia Fletcher CBE is a Professor of Competition Policy at the Centre for Competition Policy, University of East Anglia and co-editor of the Journal of Competition Law and Economics. She has been a Non-Executive Director at the UK Competition and Markets Authority (2016-2023), Financial Conduct Authority (2013-20) and Payment Systems Regulator (2014-20), and a member of Ofgem's Enforcement Decision Panel (2014-2022).

Michèle Ledger is a researcher at the Research Centre in Information, Law and Society (CRIDS) of the University of Namur where she also lectures on the regulatory aspects of online platforms at the postmaster degree course. She has been working for more than twenty years at Cullen International and leads the company's Media regulatory intelligence service.

cerre

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank
CERRE Think Tank