How EU laws cover elements in the announced Digital Fairness Act

November 2025

NEXTRADE GROUP
World trade is changing. Are you?

Table of Contents

This study is an independent report funded by the Computer & Communications Industry Association (CCIA Europe). The opinions offered herein are purely those of the author. They do not necessarily represent the views of CCIA Europe.

How EU laws cover elements in the announced Digital Fairness Act

I. Introduction

The European Union (EU) is advancing toward a new initiative, the Digital Fairness Act (DFA), which aims to tackle a broad set of harmful practices in the digital environment. In particular, the DFA is likely to address:

- Dark patterns that pressure, deceive, or mislead consumers into making choices they would not otherwise make.
- Addictive design features that exploit psychological vulnerabilities and encourage excessive use or spending, particularly among minors.
- Certain personalisation practices, such as profiling and personalised pricing deemed to unfairly exploit consumer vulnerabilities.
- Unfair price practices including "drip pricing," misleading discounts, and deceptive "starting from" prices in dynamic pricing systems.
- Digital contract management, such as complex subscription cancellations, automatic renewals, conversion of free trials into paid services without explicit consent.
- Inadequate customer service, such as excessive reliance on chatbots.
- Harmful practices by influencers, including the failure to disclose commercial partnerships and the promotion of harmful products, and clearer responsibilities for companies collaborating with influencers.

This paper seeks to support the DFA's design by reviewing how 12 flagship European Union (EU) digital, data, and consumer protection laws already address the issues that the DFA is expected to take on. This paper reaches four main conclusions:

- The EU has already tackled dark patterns in various ways. Some of these include the Digital Services Act (DSA) and Data Act's prohibitions on manipulative UI designs and dark patterns; the AI Act's ban on subliminal and exploitative techniques that distort user decision-making; the Unfair Commercial Practices Directive (UCPD)'s broad prohibition on deceptive patterns related to business-to-consumer (B2C) commercial practices; and the European Data Protection Board (EDPB) Guidelines clarifying deceptive design patterns under the General Data Protection Regulation (GDPR). The EU's existing laws also already require transparency, understandability, and accessibility, and include special protections aimed at further protecting minors and vulnerable groups.
- The DFA, if put in place, should be highly targeted and evidence-based, and only address critical and clearly identifiable gaps in existing laws.

- The DFA's enforcement should be case-by-case and focused on systematic abuses.

- Critically, any new initiative should avoid undermining the value that European consumers and SMEs are drawing from personalisation, which is shown in an accompanying Nextrade survey to have significant welfare gains for Europeans.[1]

- Where immediate action is needed, an effective enforcement mechanism could be deployed, enhancing work of the existing Consumer Protection Cooperation (CPC) network.

The following section assesses the various EU legislative instruments and how they cover the various elements that the Digital Fairness Act is expected to cover. Section three provides policy recommendations, while section four concludes.

[1] See Nextrade Group. 2025. "Survey on the personalisation of European consumers' online experience in preparation for the Digital Fairness Act." https://www.nextradegroupllc.com/digital-fairness-act-survey

II. Regulatory landscape review of existing EU and national rules related to dark patterns and personalisation

This section seeks to assess how existing EU legislation already addresses the various elements that the DFA is expected to cover. The reviewed laws include:

- **Unfair Commercial Practices Directive (UCPD)** of 2005 and subsequent amendment in 2019: addresses unfair business-to-consumer commercial practices, prohibiting misleading actions or omissions and aggressive practices that could impair a consumer's ability to make an informed decision.

- **Directive on Misleading and Comparative Advertising** of 2006: aimed to protect businesses from misleading advertising by competitors and ensure that comparative advertising is fair and does not mislead consumers.

- **Audiovisual Media Services Directive (AVMSD)** of 2010 (original, revised in 2018): sets out rules for all audiovisual media services, including traditional TV broadcasts and on-demand services, covering aspects like advertising, promotion of European works, and protection of minors.

- **Consumer Rights Directive (CRD)** of 2014: harmonises key aspects of consumer contract law across the EU, establishing rights such as information requirements for distance and off-premises contracts, and the right of withdrawal.

- **General Data Protection Regulation (GDPR)** of 2016: grants individuals extensive rights over their personal data and imposes strict obligations on organisations regarding data collection, processing, and storage.

- **European Data Protection Board (EDPB) Guidelines** ongoing from 2018: set out non-binding recommendations to ensure consistent application of the GDPR and other data protection laws across the European Economic Area.

- **Platform to Business Regulation (P2B Regulation)** of 2019: aims to create a transparent and predictable business environment for smaller businesses and traders using online platforms, addressing issues like transparency of terms and conditions, ranking, and dispute resolution.

- **Digital Services Act (DSA)** of 2022 (full application for all online platforms): aims to make online platforms accountable for the content they host, combat illegal content, and protect users' fundamental rights online.

- **Digital Markets Act (DMA)** of 2022 (full application for gatekeepers): targets large gatekeepers, imposing *ex ante* obligations and prohibitions with the goal of ensuring fair and contestable digital markets.

- **General Product Safety Regulation (GPSR)** of 2023: seeks to ensure that only safe products are placed on the EU market; impacts online sellers and platforms by extending product safety obligations to the entire online supply chain.

- **Data Act** of 2023: aims to unlock the value of data by establishing rules on who can access and use data generated by connected products or related services, promoting data sharing and interoperability.

- **AI Act** of 2024 expected to start applying in 2026: introduces risk-based law aimed to ensure that AI systems placed on the EU market are safe, transparent, and developed in a trustworthy manner.

The following provides a non-exhaustive list of examples from the various laws and guidelines in five areas considered for the DFA: combating dark patterns, addressing addictive designs, promoting transparency in personalisation, ensuring fair digital subscriptions and fairness of automated contracts, and regulating influencer marketing. Table 1 summarizes, highlighting areas with more complete coverage in darker colours.

a. Combating dark patterns

Various EU laws already address dark patterns. For example, the DSA states that "providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions."[2]

The Data Act also prohibits data holders and third parties from making the exercise of user choices or rights "unduly difficult, including by offering choices to the user in a non-neutral manner, or by coercing, deceiving or manipulating the user, or by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a user digital interface or a part thereof."[3] It specifically mentions that "third parties or data holders should not rely on so-called 'dark patterns' in designing their digital interfaces."[4] The Data Act discusses dark patterns as ways to "deceive users by nudging them into decisions on data disclosure transactions or to unreasonably bias the decision-making of the users of the service in such a way as to subvert or impair their autonomy, decision-making and choice."[5]

The AI Act prohibits AI systems that deploy "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that

[2] Article 25(1) of the DSA.
[3] Article 6(2a) of the Data Act.
[4] Recital 38 of the Data Act.
[5] Recital 38 of the Data Act.

person, another person or group of persons significant harm."[6] This includes AI systems exploiting vulnerabilities due to age, disability, or social/economic situation.[7]
The Unfair Commercial Practices Directive (UCPD) specifies that a commercial practice shall be deemed misleading if its "overall presentation" deceives, or is likely to deceive, the average consumer. This holds true even if the underlying information is factually correct, provided the practice causes or could cause the consumer to make a transactional decision they otherwise would not have.[8]

The EDPB Guidelines on Deceptive Design Patterns provide comprehensive guidance on recognizing and avoiding 'deceptive design patterns' in social media platform interfaces that infringe on GDPR requirements. These patterns aim to influence users into making unintended, unwilling, and potentially harmful decisions regarding their personal data, often in the platform's interest.[9] The guidelines discuss six deceptive design patterns, such as overloading (confronting users with a large quantity of requests), skipping (designing the interface to make users forget or overlook data protection aspects), and "left in the dark" (hiding information or controls, or leaving users unsure about data processing. Further, the EDPB draft Guidelines on the interplay between the DSA and the GDPR also refer to the effective bases already established by the current legislative framework.[10]

b. Addressing addictive designs

Many laws also address addictive designs. For example, the DSA mandates that providers of very large online platforms and very large online search engines "assess systemic risks", which include the "serious negative consequences to a person's physical and mental well-being."[11] This covers risks stemming "from online interface design that may stimulate behavioural addictions of recipients of the service." The targeted providers must take appropriate mitigating measures such as adapting the design of their service and online interface. They are also required to address gender-based violence and the protection of minors.

The GPSR states that the assessment of a product's safety should consider the health risk posed by digitally connected products, including the risk to mental health, especially of vulnerable consumers such as children. Manufacturers of digitally connected products likely to impact children must ensure their products meet the highest standards of privacy and "safety by design," which is a core requirement throughout the GPSR. It also lists "cybersecurity features necessary to protect the product against external influences, including malicious third parties, where such an influence might have an impact on the safety of the product, including the possible loss of interconnection" as a factor to consider when assessing safety.[12]

---

[6] Article 5(1)(a) of the AI Act.
[7] Article 5(1)(b) of the AI Act.
[8] Article 6(1) of the Unfair Commercial Practices Directive
[9] European Data Protection Board (2023)
[10] European Data Protection Board (2025)
[11] Recital 83 of the DSA
[12] Article 6(g) of the GPSR

c. Promoting transparency in personalisation

Many laws also have transparency obligations. The GDPR defines profiling and requires controllers to provide data subjects with information about "the existence of automated decision-making, including profiling, and meaningful information about the logic involved, its significance, and envisaged consequences."[13] The principle of transparency requires information to be "concise, easily accessible, and understandable," and that information "relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[14]

The DSA imposes significant transparency obligations on very large online platforms, for example requiring them to provide "meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters."[15] This includes explanations of the logic used, including when based on profiling. It also requires online platforms to clearly set out the main parameters of their recommender systems in their terms and conditions and explain why certain information is suggested and any options to modify or influence these parameters.[16] Very large platforms and search engines must also offer "at least one option for each of their recommender systems which is not based on profiling."

Further, the Consumer Rights Directive and the UCPD also set out certain algorithm and ranking transparency requirements on the product's interface.[17]

The AI Act emphasizes transparency as a key ethical principle for trustworthy AI. It states that "high-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately."[18] Instructions for use need to contain concise, complete, correct and clear information relevant to the deployer. They should include information on any known or foreseeable risks.[19] The recitals of the Act also have many references to transparency.

The Data Act addresses transparency too, mandating that connected products and related services be designed in such a way that data generated by their use (including metadata) is "easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user."[20] It also states that information on data holder's use of data for purposes like improving product function

---

[13] Article 13 of the GDPR.
[14] Article 12 of the GDPR.
[15] Article 26 of the DSA.
[16] Article 27 of the DSA.
[17] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights: https://eur-lex.europa.eu/eli/dir/2011/83/oj/eng
[18] Article 13 (1) of the AI Act
[19] Article 13(3)(b) of the AI Act.
[20] Article 3 of the Data Act

or developing new services must be transparent to the user, with any changes requiring informed agreement.[21]

d. Standards for digital subscriptions

The Consumer Rights Directive requires traders to provide consumers with specific information for distance contracts, including "the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract."[22] For contracts that place a consumer under an obligation to pay, the trader must make this clear and prominent before the order, and the consumer must explicitly acknowledge the obligation, with the button clearly labelled (e.g., "order with obligation to pay").[23] It also promotes clarity and transparency in consumer contracts, particularly for distance contracts and states that traders "ensure that the consumer, when placing his order, explicitly acknowledges that the order implies an obligation to pay", and labelling subscription buttons "in an easily legible manner."[24]

On its part, the Digital Services Act states that providers of online platforms should not make the process of cancelling a service "significantly more cumbersome than signing up to it."[25] Also the DMA prohibits gatekeepers from circumventing their obligations through contractual, commercial, technical, or any other means, and requires gatekeepers to "ensure that the conditions of termination can be exercised without undue difficulty."[26]

e. Automated contract fairness

The Data Act addresses "smart contracts" created by professionals for others or integrated into applications for automating data sharing agreements. It requires smart contracts to meet "essential requirements" including being able to be "interrupted and terminated" with mutual consent.[27] It clarifies that relevant civil, contractual, and consumer protection laws remain applicable to data sharing agreements even with the use of smart contracts.

The GDPR sets strict conditions for consent, requiring it to be "freely given, specific, informed and unambiguous indication of the data subject's agreement" by a clear affirmative act, not by "silence, pre-ticked boxes, or inactivity."[28] It also provides the right to withdraw consent at any time, and emphasizes that withdrawal should be "as easy as to give" consent.[29]

---

[21] Recital (25).
[22] Article 6 of the Consumer Rights Directive.
[23] Article 8 of the Consumer Rights Directive.
[24] Article 8 of the Consumer Rights Directive.
[25] Recital (67) of the DSA.
[26] Article 6(13) of the DMA.
[27] See Article 26 and Recital (104) of the Data Act
[28] Recital (32) of the GDPR.
[29] Article 7 of the GDPR.

f. Influencer marketing

The Audiovisual Media Services Directive (AVMSD) requires video-sharing platform providers to "clearly inform users where programmers and user-generated videos contain audiovisual commercial communications."[30] They must also have a "functionality for users who upload user-generated videos to declare whether such videos contain audiovisual commercial communications."[31]

The DSA requires online platforms to provide recipients of the service with "a functionality to declare whether the content they provide is or contains commercial communications."[32] If such a declaration is made, the platform must ensure that other recipients can identify it clearly and unambiguously through prominent markings.

Influencers are also classified as 'traders' under the Unfair Commercial Practices Directive (UCPD), requiring them to comply with consumer protection law provisions, in particular transparency regarding advertising and paid promotions.

This is further complemented by non-legislative guidance, such as through the European Commission's Influencer Legal Hub, which helps assist compliance and clarifies obligations for influencers and brands.[33]

Table 1 reviews how various EU mandates already cover elements that the DFA is likely to seek to focus on.

[30] Article 28(b) of Audiovisual Media Services Directive.

[31] Article 28(c) of Audiovisual Media Services Directive

[32] Article 26 of the DSA

[33] European Commission's Influencer Legal Hub: https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/influencer-legal-hub_en

Table 1 – Existing EU laws and guidelines vis-a-vis the potential elements of the Digital Fairness Act (the darker the colour, the more complete coverage)

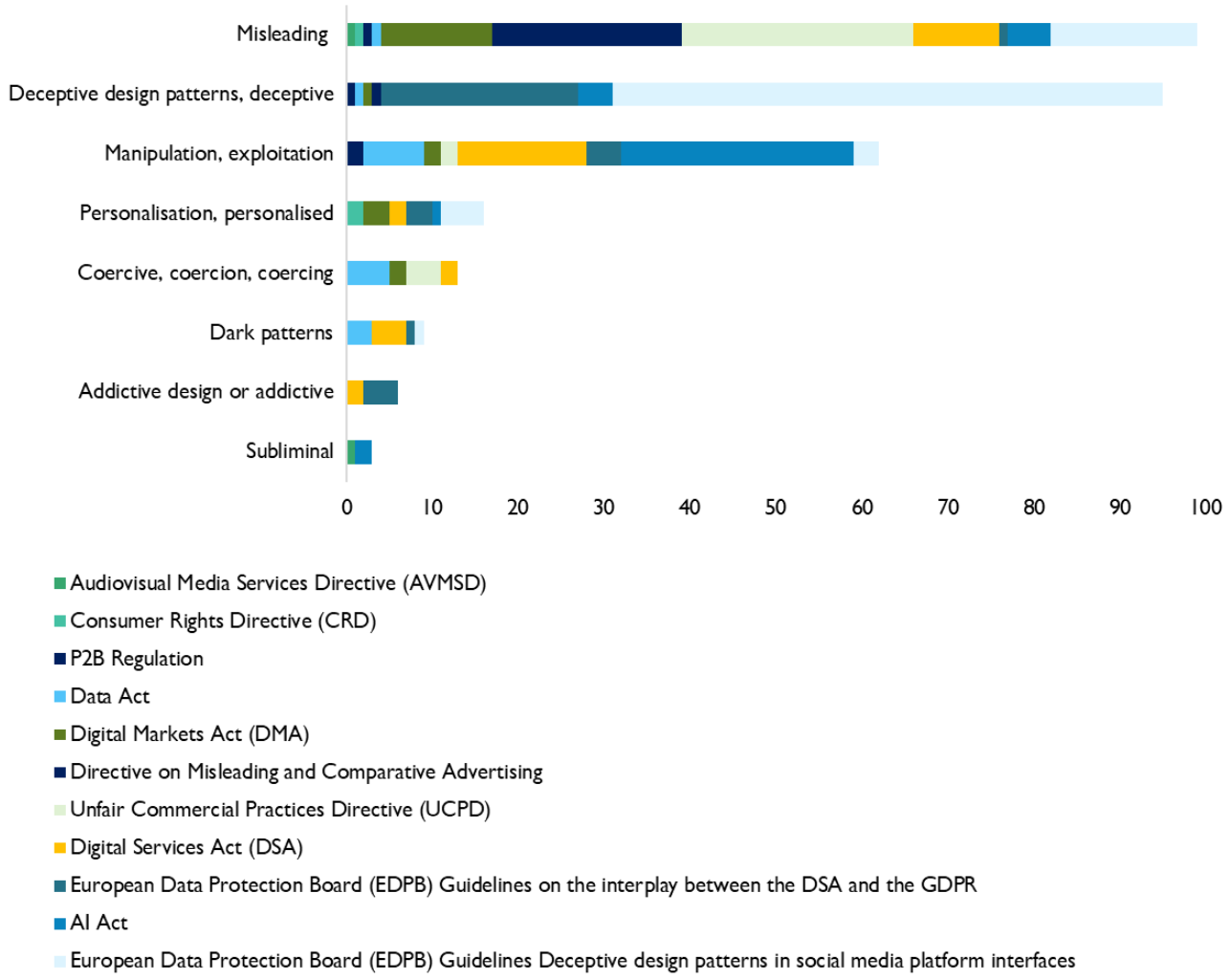
	Dark patterns and manipulative practices	Addictive design and exploitation of vulnerabilities	Manipulative personalisation	Contractual fairness and cancellations	General transparency obligations
Directive on Misleading and Comparative Advertising - 2006	No; focuses on advertising accuracy and fairness between traders.	No direct provisions on addictive design.	No	No	Permits comparative advertisement if it is not misleading.
Consumer Rights Directive (CRD) - 2011	Addresses "inertia selling," exempting the consumer from any obligation to buy.	Focuses on clear contractual terms and information requirements.	No	Yes, 14 day withdrawal.	Yes, pre-contractual information clarity.
Audiovisual Media Services Directive (AVMSD) – 2010, revised in 2018	No direct provisions on dark patterns; focuses on transparency of audiovisual commercial communications.	Requires audiovisual media services to take measures to protect minors from content that may impair their physical, mental, or moral development.	Bans the processing of minors' personal data for commercial purposes, including profiling and behaviourally targeted advertising.	No	Yes, transparency of the owners of media services.
General Product Safety Regulation (GPSR) - 2023	No direct dark pattern provisions; broadens the scope of product safety to include mental health risks posed by digitally connected products, particularly for vulnerable consumers such as children.	Indirectly - requires safety, security, and privacy by design.	No direct coverage.	No	Yes, product safety information obligations.
Unfair Commercial Practices Directive (UCPD) – 2005 and amendments in 2019	Prohibitions on fake consumer reviews and endorsements, and on manipulation of consumer reviews and endorsements.	Discusses aggressive or misleading marketing and their targeting of the elderly or vulnerable groups.	Limited; general unfair practice clauses.	Annex I contains a list of commercial practices considered misleading and unfair. Considers coercion as potentially resulting from non-contractual barriers to terminate a contract or to switch to another product or another trader.	Yes, material information needed by the average consumer.

	Dark patterns and manipulative practices	Addictive design and exploitation of vulnerabilities	Manipulative personalisation	Contractual fairness and cancellations	General transparency obligations
General Data Protection Regulation (GDPR) - 2016	Fairness and transparency and consent validity; EDPB Guidelines prohibit deceptive consent designs.	Data protection by design; EDPB Guidelines warn against manipulative patterns harming vulnerable users.	Processing requires lawful basis and transparency.	Consent for data processing must be freely given, and it must be as easy to withdraw as it is to give it.	Yes, general transparency duty.
Digital Markets Act (DMA) - 2022	Anti-circumvention prohibits interface design and subverting user autonomy (applies only to gatekeepers).	Addresses design that impairs autonomy or choice.	Prohibits combining personal data from the relevant core platform service with personal data from any further core platform services, including for ads.	Users need to be able to easily uninstall pre-installed apps or unsubscribe from core platform services.	Yes, FRAND access conditions and gatekeeper practice transparency.
Artificial Intelligence Act (AI Act) - 2024	Prohibits placing in the market AI systems that use subliminal techniques or purposefully manipulative or deceptive techniques.	Explicitly prohibits AI exploiting vulnerabilities. due to age, disability, or a specific social or economic situation	Explicitly prohibits certain AI practices that involve manipulation or exploitation.	No direct provisions.	Yes, calls for traceability and transparency.
Digital Services Act (DSA) - 2022	Explicit ban on dark patterns; compliance by design obligations. Staes that legitimate practices, for example in advertising, are not dark patterns.	Covers systemic risks including addictive design indirectly; addresses high level of privacy, safety, and security of minors in online services	Transparency of recommender systems and targeted ad bans for minors/sensitive data.	patterns, including hindering cancellations and "making the procedure of cancelling a service significantly more cumbersome than signing up to it."	Yes, Terms and Conditions' clarity, advertisement transparency, trader traceability, reporting.
P2B Regulation - 2019	No direct provisions on dark patterns; focuses on B2B fairness and transparency.	No direct coverage; focuses on B2B contractual fairness.	No	Yes, regulates fair termination conditions for business users.	Yes, transparency on differentiated treatment and complaints.
Data Act - 2023	Prohibits manipulation, including via digital interfaces; bans manipulative techniques subverting user autonomy.	Prohibits manipulative techniques can be used to persuade users, in particular vulnerable consumers, to engage in unwanted behaviours.	Provisions against misuse of data and profiling.	Yes, fair contractual terms.	Yes, various transparency obligations.

Another way to get a sense of how European legislation already pertains to dark patterns, personalisation, and transparency is to quantify mentions of them in the various laws. While by no means an exact measure of the scope of EU jurisprudence, this exercise provides a glance into the many ways in which EU's laws already address the issues the Digital Fairness Act is seeking to address – even if using somewhat different terms than "dark patterns", such as "misleading", "deceptive", or "addictive".

Existing laws and guidelines mention dark patterns and misuse many times. For example, the EDPB's two guidelines mapped here, on the interplay between the DSA and the GDPR (2025) and on deceptive design patterns in social media platform interfaces (2023) address deceptive practices such as deceptive design patterns 87 times (figure 1). European laws such as the Digital Services Act and Digital Markets Act also regulate and address various dark patterns and mandate transparency (figure 2). Laws also refer to the protection of minors dozens of times.

Figure 1 – Number of mentions of dark patterns, deceptive practices, manipulation, and similar terms in existing EU laws and guidelines



Source: Nextrade Group analysis of laws and guidelines.

Figure 2 – Number of mentions of transparency, user autonomy, protection of minors, and against manipulation and manipulative personalisation in existing EU Laws and guidelines

Source: Nextrade Group analysis of laws and guidelines.

III. Policy recommendations

As the EU continues working on the announced Digital Fairness Act, policymakers should balance protections against harmful manipulative practices with safeguards that preserve personalisation, as it is key to consumer welfare and small and medium enterprises' competitiveness. In addition, a recent Nextrade Group survey shows that European consumers are quick to abandon brands and services that are deceptive. In other words, the market rewards fairness and self-regulates against abuses.

Where immediate action is needed, an effective enforcement mechanism could be deployed, particularly for non-compliant actors, enhancing work of the existing Consumer Protection Cooperation (CPC) network.

In addition, any new regulations such as the potential DFA should also consider the numerous EU laws that already address dark patterns and mandate transparency.

There are four recommendations with regards to the upcoming DFA:

- **The Digital Fairness Act should build on the EU's existing consumer and digital regulations rather than duplicating them.** Multiple laws currently in force, such as the Digital Services Act, GDPR, and Data Act, already contain provisions that ban manipulative design practices and require transparency, consent, and fair user interface standards. The Digital Fairness Act should therefore target only clear and well-documented regulatory gaps and avoid imposing overlapping obligations that create legal uncertainty or compliance burdens, especially for SMEs.

- **Rather than establishing blanket prohibitions on data use conducive to personalisation, the Digital Fairness Act should prioritize clear, operational enforcement of the existing framework**, **clarifying the boundaries between dark patterns and permissible personalisation and design practices that benefit consumers**. It should explicitly recognize the benefits of responsible personalisation, which saves users time and enhances their digital experience.

- **The announced Act should incorporate consumer empowerment measures that emphasize transparency, informed consent, and easy opt-out or cancellation mechanisms.** Rather than imposing rigid user interface standards, the Digital Fairness Act should focus on ensuring that consumers can make decisions freely, with clear information and without undue pressure. Simplified contract terms, plain language disclosures, and easy-to-navigate consent flows should be promoted as best practices.

- **The Digital Fairness Act's enforcement should prioritize high-risk or large-scale abuses and avoid imposing a disproportionate regulatory burden on small businesses.** SMEs rely on affordable, data-driven personalisation tools to reach customers and compete with larger players. Case-by-case enforcement may be more effective than prescriptive rules, helping to tackle abusive behaviours without discouraging consumer-centric designs and offerings.

IV. Conclusion

This study, prepared to inform EU policymakers' work on the announced Digital Fairness Act, has analysed how existing European laws already regulate many of the practices the Digital Fairness Act is expected to cover.

As seen above, the existing EU legislative framework already extensively regulates manipulative designs and deceptive practices. This suggests that targeted enforcement against systematic abuses and more practical guidance should be prioritised and considered as preferable to new, broad regulations that would risk undermining personalisation and dampening innovation.

The Digital Fairness Act should be narrowly focused on genuine and evidence-based regulatory gaps and ensure consistent enforcement of existing rules across the EU, without eroding the significant benefits that personalisation brings to consumers across the board.

Critically, any new initiatives considered in the EU must ensure net benefits for both consumers and the broader digital economy by targeting harmful practices without constraining responsible personalisation.

References

European Commission. “AI Act,” 2024. https://artificialintelligenceact.eu/ai-act-explorer/.

———. “Audiovisual Media Services Directive,” 2018. https://eur-lex.europa.eu/eli/dir/2018/1808/oj.

———. “Data Act,” 2024. https://eur-lex.europa.eu/eli/reg/2023/2854.

———. “Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act),” 2022. https://www.eu-digital-services-act.com/Digital_Services_Act_Article_25.html.

———. “Digital Markets Act.” Europa.eu, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC.

———. “Directive - 2011/83 - EN - Consumer Rights Directive - EUR-Lex.” Europa.eu, 2011. https://eur-lex.europa.eu/eli/dir/2011/83/oj/eng.

———. “General Data Protection Regulation,” April 27, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

———. “General Product Safety Regulation,” 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.135.01.0001.01.ENG&toc=OJ%3AL%3A2023%3A135%3ATOC.

———. “Platform-to-Business (P2B) Regulation,’,” 2019. https://eur-lex.europa.eu/eli/reg/2019/1150/oj/eng

_____. “Public Consultation on the Digital Fairness Act.” European Commission - Have your say, 2025. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14622-Digital-Fairness-Act_en.

———. “Unfair Commercial Practices Directive,” 2005. https://eur-lex.europa.eu/eli/dir/2005/29/oj/eng.

European Data Protection Board. “Guidelines 3/2025 on the Interplay between the DSA and the GDPR Version 1.1,” 2025. https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf.

———. “Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces,” 2023. https://www.edpb.europa.eu/system/files/2023-02/edpb_03-

2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

Nextrade Group. 2025. “Survey on the personalisation of European consumers’ online experience in preparation for the Digital Fairness Act.” https://www.nextradegroupllc.com/digital-fairness-act-survey