EUROPEAN
COMMISSION

Brussels, 3.10.2024
SWD(2024) 230 final

COMMISSION STAFF WORKING DOCUMENT

FITNESS CHECK

of EU consumer law on digital fairness

{SEC(2024) 245 final} - {SWD(2024) 231 final}

Table of Contents

1. Introduction 1
2. What was the expected outcome of the intervention? 3
2.1 Description of the intervention and its objectives 3
2.2 Points of comparison 7
3. How has the situation evolved over the evaluation period? 11
Consumer participation in digital markets 11
Consumer awareness of their rights 14
Consumer complaints in the context of digital growth 14
Scale of specific problems 17
Financial consumer detriment quantified 24
Other harms 29
Implementation and application 33
4. Evaluation findings 35
4.1. To what extent was the intervention successful and why? 35
4.1.1. Effectiveness 36
4.1.1.1. Achievement of the objectives 36
4.1.1.2. Competitiveness, innovation and impact on SMEs 40
4.1.1.3. Legal uncertainty and limitations 44
Legal uncertainty 44
Standard of consumer behaviour 45
4.1.1.4. Enforcement 48
Insufficient enforcement 48
Public enforcement and the CPC network 49
Enforceability of substantive law 51
4.1.2. Coherence 55
4.1.2.1. Internal coherence 55
4.1.2.2. External coherence 55
Consumer protection reinforcements (DSA, DMA, Data Act, AI Act) 56
Regulatory complexity 58
Implementation and enforcement 60
Remaining challenges 62
4.1.3. Efficiency 65
4.1.3.1. Business benefits and costs 65
Overview of benefits 65

Costs related to the Directives ... *67*
Costs from the lack of EU-level harmonisation ... *72*
4.1.3.2. Impacts on consumers ... *73*
4.1.3.3. Impacts on consumer authorities ... *74*
4.1.3.4. Scope for simplification and burden reduction ... *76*
4.2. How did the EU intervention make a difference and to whom? ... 79
4.3. Is the intervention still relevant? ... 80
Current and emerging needs ... *80*
Technological developments ... *82*
Safety-net framework ... *85*
5. What are the conclusions and lessons learned? ... 85
Annex I: Procedural Information ... 91
Annex II. Methodology and Analytical models used ... 100
Annex III. Evaluation matrix ... 110
Annex IV. Overview of benefits and costs ... 122
Annex V. Stakeholders consultation - Synopsis report ... 128
Annex VI. Analysis of problematic practices ... 146
VI.1. Problematic practices ... *146*
VI.1.1. Dark patterns ... *14*
VI.1.2. Addictive design and gaming ... *153*
VI.1.3. Personalisation (advertising, ranking, recommendations, pricing/offers) ... *162*
VI.1.4. Social media commerce and influencer marketing ... *169*
VI.1.5. Contract cancellations and digital subscriptions ... *176*
VI.1.6. Unfair contract terms ... *182*
VI.1.7. Automated contracting ... *195*
VI.2. Other problems ... *200*
VI.2.1. Dropshipping ... *200*
VI.2.2. AI chatbots ... *200*
VI.2.3. Scalper bots ... *202*
VI.2.4. Ticket sales ... *202*
Annex VII. External coherence – list of provisions relevant for consumer protection ... 204
Digital Services Act ... 204
Digital Markets Act ... 207
Data Act ... 209
AI Act ... 210

Notice

The information herein is of a general nature only. Neither the European Commission nor any person acting on behalf of the European Commission is responsible for any use that may be made of the following information.

The views expressed therein cannot prejudge the position that the European Commission might take before the Court of Justice of the European Union. Only the text of the Union legislation itself has legal force. Any authoritative reading of the law has to be derived from the text of the legislation and directly from the decisions of the Court of Justice of the European Union.

The views are without prejudice to any guidance that the European Commission may adopt in the future in relation to the legislation.

The Fitness Check takes into account developments until June 2024.

Glossary

Acronym	*Meaning or definition*
AI	Artificial intelligence
ADR	Alternative dispute resolution
AVMSD	Audiovisual Media Services Directive
B2B	Business-to-business
B2C	Business-to-consumer
BEUC	Bureau Européen des Unions de Consommateurs (European Consumer Organisation)
CBA	Cost-Benefit Analysis
CCD	Consumer Credit Directive
CCS	Consumer Conditions Scoreboard
CPAs	Consumer Protection Authorities
CPC	Consumer Protection Cooperation Network
CRD	Consumer Rights Directive
DCD	Digital Content Directive
DMA	Digital Markets Act
DMFSD	Distance Marketing of Financial Services Directive
DSA	Digital Services Act
ECC	European Consumer Centre
GDPR	General Data Protection Regulation
IoT	Internet of Things
MD	Modernisation Directive (also known as the Omnibus Directive)
MS	Member State
PLD	Product Liability Directive
T&C	Terms and Conditions

UCPD	Unfair Commercial Practices Directive
UCTD	Unfair Contract Terms Directive
VLOP	Very large online platform
VLOSE	Very large online search engine

Term	***Meaning or definition***
Dark patterns	Unfair commercial practices deployed through the structure, design or functionalities of digital interfaces or system architecture that can influence consumers to take decisions they would not have taken otherwise
Dropshipping	Sale of products without the seller holding the products in stock; the order is generally passed to a supplier (wholesaler or producer) and to other traders for delivery and returns, without the seller's direct involvement
Influencers	Persons engaging in commercial practices with an ability to affect the behaviour, opinion and purchase decisions of consumers due to their authority, knowledge, position or relationship with their audience
In-app currencies	Virtual currencies (excluding crypto currencies or digital forms of central bank money) used in apps such as video games and social media as a type of payment to acquire virtual items or other products/services
Loot boxes	Virtual items that contain uncertainty-based rewards (e.g. opening a mystery box to obtain other virtual items), generally used in video games
Scalper bots	Software to automatically purchase products in high demand with a view to reselling them at a higher price
Virtual items	Items or features within an app (e.g. video game) that a consumer can purchase to use or trade in that online environment (e.g. gifts, cosmetic features, loot boxes, card packs)

1. Introduction

Purpose and scope of the fitness check

EU consumer protection laws aim at empowering consumers to play an active role and fully benefit from the Digital Single Market. However, the digital transition is introducing both improvements and challenges to business-to-consumer markets. There are increasing concerns that new technologies and data-driven practices are used to undermine consumer choice and to influence them to take decisions that go against their interests. This could reduce consumer trust and limit the effectiveness of the current rules in the digital environment.

In response to the **emerging concerns about the lack of digital fairness for consumers**, the Commission announced in the New Consumer Agenda of 13 November 2020 that it will analyse whether additional legislation or other action is needed in the medium-term in order to ensure equal fairness online and offline. The 2021 Council Conclusions on the New Consumer Agenda highlighted the need to ensure a reliable, safe and fair digital environment for consumers through, among others, future-proof legislation that takes into account the challenges posed by the digital era.

As a first follow-up action, the Commission updated its guidance documents to explain how existing EU consumer law instruments can be used to their full potential in the digital environment. The new Commission Notices on the interpretation and application of the Directives were published in the Official Journal on 29 December 2021. As a second step, in May 2022 the Commission launched a Fitness Check of EU consumer law on digital fairness in order to determine whether the existing key horizontal consumer law instruments remain adequate for ensuring a high level of consumer protection in the digital environment (digital fairness) or whether any changes are necessary. The Fitness Check was included in the 2024 Commission Work Programme.

A Fitness Check is a comprehensive evaluation of a policy area that addresses the extent to which a set of related EU legislative acts have contributed or not to attaining EU policy objectives. It is well suited to identifying regulatory overlaps, inconsistencies, synergies, digitalisation potential and cumulative impacts. This **Fitness Check covers three Directives**, which form the core of the framework of consumer protection that applies to most traders and consumer-facing sectors in the EU:

- Unfair Commercial Practices Directive 2005/29/EC (UCPD);
- Consumer Rights Directive 2011/83/EU (CRD);
- Unfair Contract Terms Directive 93/13/EEC (UCTD).

For the purposes of this Fitness Check, the Commission uses the concept of 'digital fairness' to refer to a high level of consumer protection, enshrined in Article 169 TFEU, that should be ensured in the digital environment, in compliance with the legal standards established in EU consumer law.[1] This Fitness Check builds on the findings of the 2017 Fitness Check of EU consumer law and 2017 CRD evaluation, which confirmed that, in general, EU consumer law was deemed fit for purpose but identified the need for targeted legislative changes to strengthen the existing framework, including in the digital area, and to improve its enforcement. Taking into account the fast pace of developments in digital markets and the increase in EU legislation in the digital sector since 2017, it was deemed necessary to undertake a new Fitness Check with

[1] For example, in order for a contract term to be fair under the UCTD, it should not cause a significant imbalance in rights and obligations to the detriment of the consumer; in order for a commercial practice to be fair under the UCPD, it should not breach the prohibitions contained therein and to materially distort the economic behaviour of the average or vulnerable consumer.

a specific focus on new digital practices that may create problems from the consumer protection perspective. In contrast to the previous Fitness Check, this evaluation **focuses only on how the Directives are applied in the digital environment** and the specific challenges raised by digitalisation as regards consumer protection. Therefore, the evaluation findings laid out in this report, including any estimates on consumer detriment and business costs, relate only to the online, not offline, context.

The **evaluation period chosen (2017-2023)** enables the Commission to complete a comprehensive assessment that takes into account the entry into application of the latest changes to these Directives on 28 May 2022 by the Modernisation Directive and the 2018 Impact Assessment accompanying that Directive. This period also covers several enforcement activities in the digital area and other legislative developments concerning EU legislation that interplay with EU consumer law, such as the Audiovisual Media Services Directive (AVMSD), Digital Services Act (DSA), Digital Markets Act (DMA), Artificial Intelligence Act (AI Act) and Data Act. This new legislation - despite important differences in scope and nature - will undoubtedly have implications for consumer protection. However, several of these laws have only just entered into force, as a result of which their likely impact cannot be fully reflected yet. For example, in view of the entry into application of the obligations under the DSA and DMA in the course of 2023 following the respective designations of very large online platforms/very large online search engines (VLOPs/VLOSEs) under the DSA and gatekeepers under the DMA, the assessment of the impact of these rules cannot be comprehensive. Furthermore, the Data Act and AI Act have not yet fully entered into application, as a result of which their practical effects cannot be assessed during the evaluation period.

The Fitness Check covers the **five key evaluation criteria** specified in the Better Regulation guidelines, namely effectiveness (progress towards achievement of objectives), efficiency (cost-effectiveness and proportionality of costs to benefits, potential for simplification), relevance (to current and emerging needs, fitness for purpose given regulatory and technological developments), coherence (internal and external with other EU or Member States' interventions) and EU added value (producing results beyond what would have been achieved by the Member States acting alone). The Fitness Check is **primarily retrospective in focus**; however, there is a forward-looking aspect to assess the ongoing relevance and 'fitness for purpose' of the Directives.

The geographical scope of the Fitness Check covers the EU, however, for efficiency reasons, certain data collection activities (sweeps, consumer survey, business survey) cover only ten Member States (DE, EE, ES, FR, IT, HU, PL, PT, RO, SE). The results can be considered representative in terms of sample size, covering different EU regions and allowing, to the extent possible, extrapolation to the EU. Specific research activities also include an international dimension to ascertain the extent to which problematic practices are prevalent and regulated outside of the EU. The methodology for the evaluation entails a variety of techniques and data sources, including extensive consultations of relevant stakeholders and a supporting study carried out by external contractors.

The Fitness Check's conclusions outline the broad categories of issues identified and possible solutions that emerged during the evaluation - while refraining from prejudging any future prioritisation of issues and the content or format of the follow-up actions (including any future impact assessment of possible concrete measures).

2. What was the expected outcome of the intervention?

2.1 Description of the intervention and its objectives

The Directives assessed in this Fitness Check primarily aim at protecting the economic interests of consumers. The Treaties (Articles 114 and 169 TFEU) and the Charter of Fundamental Rights (Article 38) require a **high level of consumer protection**, which is the main general objective of the UCTD, UCPD and CRD. Furthermore, the Directives also contribute to the general objective of the **proper functioning of the Internal Market** by harmonising certain aspects of Member States' laws, regulations and administrative provisions. The Directives were adopted over the last three decades; the UCTD became applicable in all Member States from 31 December 1994, the UCPD from 12 December 2007 and the CRD from 13 June 2014. With the exception of the CRD, which regulated distance contracts, at the time of adoption, these Directives were not specifically focused on digital practices. Moreover, there were no specific monitoring indicators established concerning their performance in the digital environment.

Objectives of the Unfair Contract Terms Directive: The UCTD aims to protect consumers against the use by traders of not individually negotiated contract terms which, contrary to the requirement of good faith, create a significant imbalance in the parties' rights and obligations to the detriment of the consumer. The Directive provides that unfair terms are not binding on the consumer. It applies both online and offline, as well as to all products, including digital products and services. It contains, in its Annex, an indicative and non-exhaustive list of terms that may be considered as unfair, which aims at guiding the national authorities and courts in their case-by-case assessment of a contract term by listing some of the most common types of potentially unfair terms. It is a minimum harmonisation instrument and Member States can lay down stricter consumer protection rules in their national legislation. Many Member States have used this possibility by, for example, introducing blacklists of contract terms considered unfair in all circumstances. The UCTD also contains transparency requirements to the effect that contract terms have to be in plain, intelligible language. The specific objectives of the UCTD are therefore protecting consumers against unfair contract terms, and ensuring that contract terms are expressed in a clear and intelligible manner.

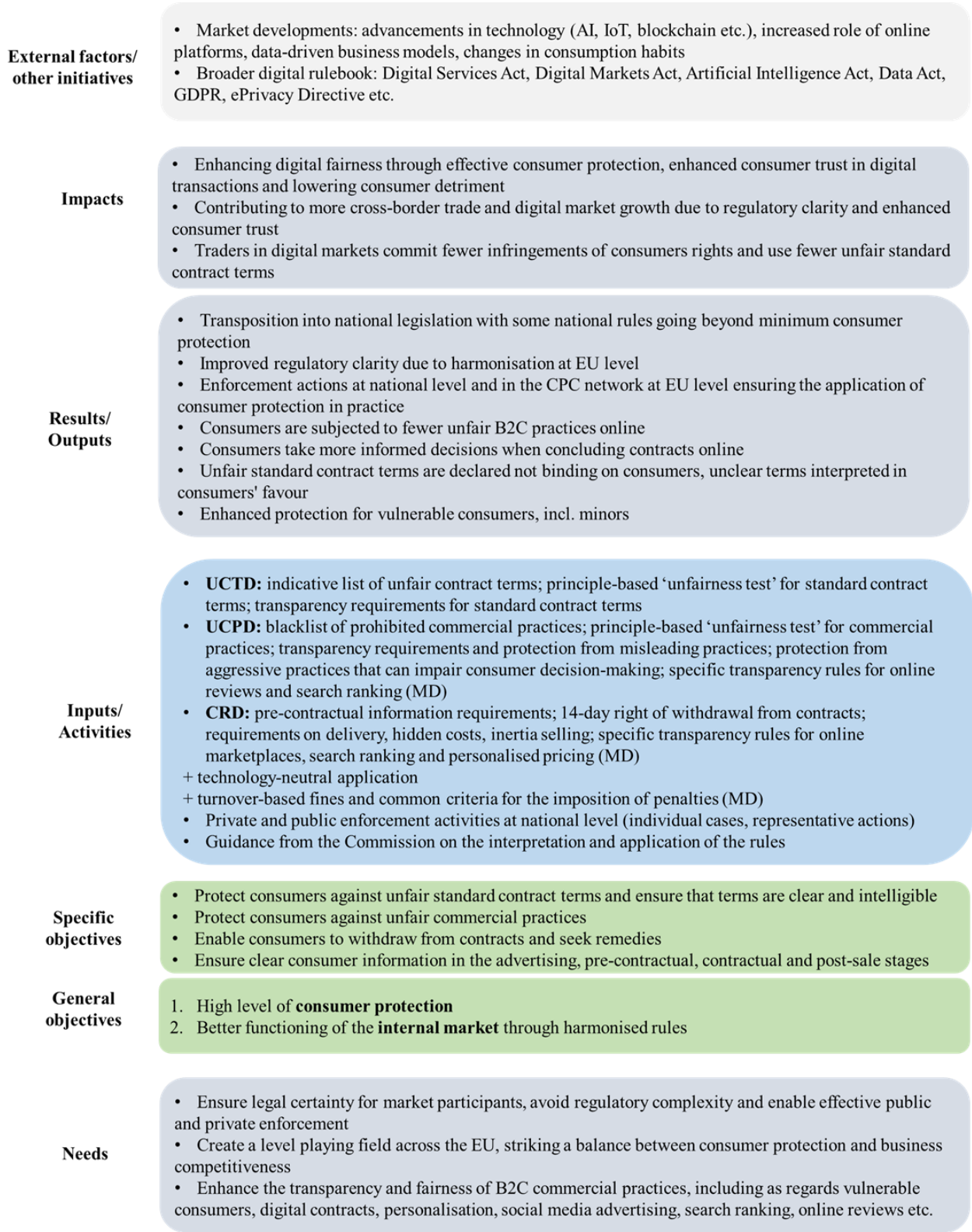
Objectives of the Unfair Commercial Practices Directive: The UCPD aims to protect consumers against unfair business-to-consumer commercial practices by traders before, during or after a transaction, including in the digital environment. It applies to all products, including digital products and services. The Directive provides, in principle, for full harmonisation, subject to exceptions, such as the rules on financial services and immovable property. The Directive provides, in its Annex I, a blacklist of specific commercial practices which are prohibited in all circumstances and in Articles 5-9 prohibits commercial practices which are considered as contrary to the requirements of professional diligence, misleading or aggressive. With the exception of the practices in the blacklist, it must be demonstrated that a commercial practice causes or is likely to cause an average or vulnerable consumer to take a transactional decision that they would not have taken otherwise. The specific objectives of the UCPD are therefore protecting consumers against unfair commercial practices by prohibiting specific business practices, and ensuring better consumer information in the advertising, contractual and after-sale stages.

Objectives of the Consumer Rights Directive: The CRD aims to provide specific protection concerning B2C contracts for goods and services, including digital content and digital services. It is, in principle, a full harmonisation Directive but allows Member States in certain cases to impose additional rules as, for example, with respect to pre-contractual information

requirements for on-premises contracts (Article 5(4)). The CRD also contains a number of regulatory choices. The CRD provides for pre-contractual information requirements and specifies some of the related formal requirements. It also introduces a 14-day right of withdrawal from distance or off-premises contracts, that consumers can exercise without giving any reasons (subject to certain exceptions) or incurring any costs (other than those specified, such as, for example, the cost of sending the goods back). The CRD also sets out several other consumer rights, namely regarding the termination of the sales contract (unless agreed otherwise, the delivery should take place no later than 30 days from the conclusion of the contract). It prohibits charging consumers fees for the use of a given means of payment and requires the costs of communication by a consumer with a trader by telephone to not be more than the basic rate, as well as the consumer's express consent for any extra payments. The specific objectives of the CRD are therefore ensuring better consumer pre-contractual information, providing an effective 14-day right of withdrawal, and protecting consumers against delivery problems, hidden costs and unsolicited supply.

The Fitness Check is guided by a digital-specific **intervention logic** of the three Directives (see graph below), which explains the rationale for the interventions, adapted to the digital environment.

Figure 1 - Intervention logic for the UCTD, UCPD and CRD in the digital environment



Source: DG JUST

The UCPD and UCTD contain general clauses ('**principle-based approach**') that are used by national courts and authorities to assess the unfairness of commercial practices and contract terms used by traders on a case-by-case basis. In contrast, the CRD is more prescriptive in nature. The main benefit of the principle-based approach is to retain flexibility in the legal

framework, which can evolve over time and cover new problems that were not initially foreseen when the Directives were adopted. However, this approach entails a lack of legal certainty for consumers and traders about what rights and obligations exist. Furthermore, it may take several years for case law to emerge in response to new digital practices, causing legal uncertainty in the interim. Furthermore, interpretations in case law and enforcement actions could entail divergences and contradictions to a certain degree. The principle-based approach is hence complemented by an exhaustive list of commercial practices that are always prohibited (UCPD blacklist) and by an indicative and non-exhaustive list of unfair contract terms (UCTD indicative list), which facilitates more effective enforcement.

The UCPD and CRD are, in principle, **full harmonisation** Directives (subject to exceptions), which means that Member States may not maintain or introduce in their national legislation provisions that are not in line with the Directives, unless the Directives provide otherwise. This is the case even if the national measures are intended to provide a higher level of consumer protection, for example by regulating new problematic digital practices. In contrast, the UCTD is a **minimum harmonisation** Directive, leaving Member States more flexibility to respond to new developments.

The UCPD, CRD and UCTD are generally **technology-neutral**, meaning that the rules apply to all types of traders, commercial practices, products and services, regardless of the underlying technology or business model that is used, unless specified otherwise in specific provisions. The main benefit of their general principle-based provisions is that they are sufficiently broad to cover also new market developments. However, a disadvantage of such rules is that they might be interpreted and applied differently by market players in the context of new technological developments. They are, therefore, less effective in terms of ensuring legal certainty than more specific and detailed rules.

In order to enhance legal certainty, to assist courts and enforcement authorities, as well as to raise awareness among all market participants, the **Commission has issued guidelines** on the interpretation and application of the Directives: UCPD Guidance[2] (updated in 2021), CRD Guidance[3] (updated in 2021) and UCTD Guidance[4] (adopted in 2019). These guidelines give examples of European and national case law, and the Commission's view of how the legislation should be applied in the digital environment. For example, section 4.2 of the UCPD Guidance document focuses entirely on the digital sector and addresses issues such as the obligations of online platforms, the ranking of search results, consumer reviews, data-driven practices, dark patterns and influencer marketing. However, the Commission's guidelines are not legally binding and, as such, their impact on the levels of compliance is difficult to ascertain. Ultimately, any authoritative reading of the law can only be derived from the text of the Directives and from the case law of the Court of Justice of the EU.

Since the Directives assessed in this Fitness Check apply horizontally across most economic sectors and cover many aspects of business-to-consumer transactions, there are several points of **interaction with other EU legislation**. The interplay between the different EU legal instruments is regulated by the *lex specialis* principle (Art. 3(4) UCPD, Art. 3(2) CRD), whereby the provisions of these general EU consumer law instruments apply when the relevant

[2] Commission Notice - Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021/C 526/01) (OJ C 526, 29.12.2021, p. 1–129).
[3] Commission Notice - Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights (2021/C 525/01) (OJ C 525, 29.12.2021, p. 1–85).
[4] Commission Notice - Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts (2019/C 323/04) (OJ C 323, 27.9.2019, p. 4–92).

aspects of the B2C transactions are not more specifically regulated by the provisions of sector-specific EU law. In case of conflict between the provisions of the Directives and other EU legislation regulating specific aspects of B2C transactions, the latter would generally prevail and apply to those specific aspects. The UCTD is complementary to sector-specific EU law and applies in parallel, unless explicitly excluded. Consequently, the horizontal consumer law **Directives work as a safety net**, ensuring that a high level of consumer protection can be maintained in all sectors, including by complementing and filling possible gaps in other EU legislation in the digital area.

2.2 Points of comparison

This Fitness Check focuses on main developments from 2017 to 2023, i.e. since the conclusion of the previous 2017 Fitness Check of EU consumer law[5] and 2017 CRD evaluation[6], which examined the three Directives in their entirety, without specifically focusing on the digital environment. The situation described in these evaluations is taken as a point of comparison for the purpose of this Fitness Check.[7]

In summary, the 2017 evaluations indicated that the Directives were **partially effective**; however, as the **number of consumer complaints remained at similar levels between 2008 and 2016**, it was concluded that there was no significant progress in traders' compliance with consumer law. The evaluations pointed in particular to **insufficient enforcement**, including **limited awareness** and redress possibilities, but considered the legal framework to be broadly fit for purpose, with **scope for targeted strengthening**, including in the digital area. These evaluations led to the 2018 New Deal for Consumers package, including the Modernisation Directive, which introduced targeted amendments to the three Directives. The package included a second proposal for a directive that was adopted later as Directive (EU) 2020/1828 on Representative Actions[8].

For the purposes of this Fitness Check, the main **indicators of success**, which relate to both the general and specific objectives of the three Directives, include:

- number of reported consumer problems related to commercial practices in the digital environment and their magnitude, including any detriment suffered;
- levels of consumer trust in traders when using digital services and products or shopping online and cross-border;
- levels of awareness of consumer rights applicable in the digital environment;
- number and content of case law and enforcement actions based on the three Directives at European and national level in the digital area;[9]

[5] 'Results of the Fitness Check of consumer and marketing law and of the evaluation of the Consumer Rights Directive', 29.05.2017.

[6] Report from the Commission to the European Parliament and the Council on the application of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, 23.05.2017 (COM(2017) 259 final).

[7] UCTD and UCPD pre-date the Better Regulation guidelines and were not accompanied by Impact Assessments with monitoring indicators for the general and specific objectives described earlier. The 2008 Impact Assessment accompanying the CRD did not include monitoring indicators and the material scope of the proposed Directive changed significantly in the course of legislative negotiations.

[8] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).

[9] In principle, a lower volume of case law and enforcement actions could indicate a lack of problems and a reduction in consumer detriment. However, this is unlikely to be the case in the area of consumer protection, which is characterised by the inactivity of individual consumers in filing complaints and disproportionate barriers to taking enforcement action, compared

- compliance costs for businesses, in particular for SMEs, concerning commercial practices in the digital environment;
- perceptions of the effectiveness and clarity of the legal framework for all parties concerned in the digital area (e.g. consumers, traders, enforcers, courts);
- perceptions of the extent to which they create a level playing field by harmonising consumer laws in the digital area, preventing regulatory fragmentation.

Additional information about the relevant indicators, per evaluation question, is provided in Annex III in the evaluation matrix.

The 2018 impact assessment accompanying the New Deal for Consumers package included certain monitoring indicators that can be used, by analogy, for evaluating the progress made towards the objectives of the three Directives in the digital context. The progress based on these monitoring indicators is presented in the table below:

Table 1 - Monitoring indicators from the 2018 Impact Assessment on the Modernisation Directive

Monitoring indicator	**Baseline (2016/2017)**	**Target[10] (2027)**	**Most recent data**
% of consumers having experienced any problem when buying or using any goods or service (where they thought they had a legitimate cause for complaint)	20.1%	15%	30%[11] **(online purchases)*
% of consumers feeling confident purchasing goods or services via the Internet from retailers or service providers in other EU country	57.8%	70%	43%[12]
% of retailers thinking that differences in national consumer protection rules constitute an obstacle to the development of online sales to other EU countries	37.4%	25%	36%[13]

Source: DG JUST, based on data from the CCS and retailers survey

As indicated in the table, there has not been sufficient progress towards achieving the targets that the Commission established. In particular, **the incidence of consumer problems in online purchases is 200% higher than the 2027 target for all purchases**. However, these figures have to be put into context, including the entry into application of the second legislative proposal of the 2018 review package (Directive (EU) 2020/1828) only in June 2023, and take into account the exponential growth of digital markets and other factors. It should also be noted that the use of consumer complaints as a proxy for consumer detriment has inherent limitations. In particular, complaint figures rely on consumer perceptions of problems, which are likely to underestimate the real scale of infringements since many consumers that experience problems

to the amount of harm suffered. Against this background, a higher number of case law and enforcement action based on the three Directives would rather indicate success and additionally contribute to increasing the clarity of the legal framework through its practical application in specific cases.

[10] In 5 years after the entry into application of the MD, i.e. by 28 May 2027.

[11] 2023 Consumer Conditions Scoreboard. 30% of consumers who purchased online faced problems, compared to the overall figure of 25% of consumers facing problems if online and offline are combined.

[12] Consumer Conditions Scoreboard 2021 – Consumer Conditions Survey: Consumers at home in the single market – 2021 edition. The last available data is from 2021 because this question was discontinued in the survey. Additional data from the consumer survey for this Fitness Check (2023) on whether consumers are confident navigating the internet and using digital tools and services shows that 17% of consumers are confident, 47% somewhat confident, 25% a little confident, 7% not confident at all, 4% don't know. Additionally, when asked about trust in online businesses and websites, 6% of consumers were very trusting, 43% somewhat trusting, 37% a little trusting, 9% not at all trusting, 5% don't know.

[13] Consumer Conditions Scoreboard 2019 – Consumers at home in the single market – 2019 edition. The last available data is from 2019 because the bi-annual retailers survey was discontinued that year.

do not make official complaints. Furthermore, consumers may experience detriment but could be unaware that it has occurred (e.g. overpaying for a product due to a dark pattern or hidden advertising by a social media influencer) or may lack knowledge about the applicable laws. Nevertheless, consumer complaint figures have been a key indicator in the area of EU consumer protection policy already prior to the 2017 Fitness Check and make it possible to measure progress over time, alongside other indicators. Section 3 will analyse the evolution of the problems with more granularity.

Additional points of comparison concern the two quantitative figures provided in the 2017 Fitness Check: the amount of financial consumer detriment resulting from traders' non-compliance with the laws and the business costs related to compliance activities. Both figures are estimations and not an exact match as a baseline for the purposes of this Fitness Check, given differences in scope. In order to ensure comparability, the 2017 figure refers to the share of online detriment. In particular, Section 3 and Annex II explain the necessary adaptations that had to be carried out to establish a more appropriate baseline based on the initial figures for consumer detriment. The progress based on these new, adapted indicators is presented in the table below.

Table 2 - Additional indicators with adapted estimations comparable to the data from the 2017 Fitness Check

Indicator	**Baseline (2016/2017)**	**Target**	**Most recent data (2023)**
Estimation of post-redress financial detriment suffered by consumers as a result of problems online	EUR 3.9 billion[14]	Reduction of detriment	EUR 7.9 billion
Estimation of total annual compliance costs for traders	No direct baseline; only comparable figure from the 2017 Fitness Check - EUR 278 million **(covering only five economic sectors and excluding CRD related costs)*	Stability in the order of magnitude of costs	EUR 511-737.3 million **(covering all digital sectors)*

Source: DG JUST, based on data from the 2017 Fitness Check compared to this Fitness Check (including data from Eurostat, CCS, consumer and business surveys)

As indicated in the table, there has not been sufficient progress towards reducing financial consumer detriment. However, the magnitude of compliance costs has remained stable over the evaluation period (taking into account the limitations of comparability with the previous baseline figure, which had a more restricted scope).

Remarks on methodology and the robustness of evidence

The Fitness Check relies on a mixed method approach, which included an external supporting study and the collection of complementary sources of information over the course of two years, including extensive consultations of the public and all relevant stakeholders (i.e. through surveys, interviews, events, Member State and stakeholder Expert Group meetings), observational market data, behavioural insights, desk research, case studies, compliance sweeps and quantitative data on key effects extrapolated to the EU27 (consumer detriment and business costs). The information gathered has been triangulated/cross-checked to identify points of consensus and disagreement, allowing further analysis of the reasons behind these findings.

[14] See the calculations in Section 3 on the creation of an online-specific baseline.

The Fitness Check complied with all of the necessary elements of the Better Regulation Guidelines, such as completing an analysis of all five evaluation criteria (effectiveness, efficiency, coherence, relevance, EU added value), allocating sufficient time for the evaluation process, looking at simplification and burden-reduction potential as part of the efficiency analysis, conducting broad consultations of all relevant stakeholders and examining possible regulatory overlaps, inconsistencies and synergies across the broader EU regulatory framework applicable to the digital environment. Quantitative data sources were triangulated with other comparable data in order to validate the order of magnitude of the results. The consumer surveys referred to in this report reflect over 37 000 consumer experiences, while the business survey covered the direct responses of 1000 businesses of which 77% were SMEs, in addition to the feedback received from EU-level trade associations that represent hundreds of thousands of businesses operating in B2C digital markets.

Nevertheless, the quality of the evidence base should be seen in the context of various objective limitations:

- ***The degree to which the evidence gathered in the EU consumer policy area is qualitative, primarily opinion-based**, with the usual limitations and uncertainties associated to this type of data. The reliance on Commission-run surveys is necessary due to the absence of reporting requirements in the Directives and the lack of longitudinal datasets from public or private sources (e.g. limited market sweeps by authorities; no automated monitoring solutions) on the very wide range of issues covered by the Directives' material scope. In terms of survey limitations, it is noted that the targeted stakeholder survey was more industry-dominated, with over 50% of participants representing traders or trade associations. Furthermore, the public consultation generally cannot be considered to be a representative survey, in particular due to its sample size. However, representative views were obtained through the consumer survey and business survey, which cover a sufficient sample size, ensuring geographical balance and the possibility to extrapolate to the EU. In the report, there is a conscious balance between using data from the different surveys, to ensure neutrality. Furthermore, questions on which there was major divergence among respondents have been outlined in the report. The report did not rely on the consumer survey or consumer responses to the public consultation as regards legal assessment questions.*
- ***The limited availability of appropriate quantitative data, in particular as regards the ability to measure progress over time**. Whilst the findings of the different surveys conducted as part of this Fitness Check enabled to estimate the current consumer detriment in relation to problematic digital practices (including in quantitative terms), there do not exist specific detriment figures specifically about the application of the three Directives in the digital context at the start of the evaluation period. However, it was possible to produce a baseline retrospectively and changes were put into the context of e-commerce growth and inflation, among other factors. Additional sources of data about consumer detriment from 2017 were sought out to triangulate and verify the results. However, while some of the practices already existed at the start of the evaluation period (e.g. influencer marketing, dark patterns), others emerged only recently (use of AI chatbots) or are still emerging in B2C markets (e.g. virtual worlds). There are also specific limitations regarding data collection at European and national level concerning the amount of consumer complaints, case law and enforcement activities. Quantitative court data and statistics are either not available in most Member States or do not provide a sufficient level of detail that would enable to understand the legal provisions/Directives at stake or to distinguish between online and offline scenarios. The consequence of the unavailability of data has the effect that the estimates given in this Fitness Check are likely to be conservative and underestimate the scale of the problems. The limitations related to monitoring also stem from the lack of previous Impact Assessments and precise monitoring indicators relevant for the three Directives in the digital context. The UCTD and UCPD pre-date the Better Regulation guidelines. The 2008 Impact Assessment accompanying the CRD did not include monitoring indicators and the material scope of the proposed Directive changed significantly in the course of legislative negotiations.*
- ***The objective difficulty of attributing the benefits and costs to the specific rights and obligations stemming from the three Directives**. While stakeholder feedback gathered for the purpose of this Fitness Check clearly points to a strong link between the application of the three Directives and the effectiveness of consumer protection in the digital environment, it is not possible to directly attribute all of these changes to the Directives or to their specific provisions. To reduce administrative costs, the Directives do not include any reporting requirements for traders or Member States (beyond the standard requirement to notify the Commission of the national transposition rules). National administrations and EU businesses therefore do not have customised accounting systems regarding their costs or benefits, which means there is a need to rely on the estimates provided during interviews and in surveys. When examining business costs, multi-channel traders found it difficult to disentangle compliance costs associated with digital channels from offline channels and most traders are unable to isolate costs for their obligations regarding the three Directives specifically from those concerning, for example, product labelling or safety*

requirements. More generally, as the Directives apply to both online and offline environments, there are limitations regarding the extent to which it is possible to disentangle the 'digital' impacts and costs. A digital-specific intervention logic, baseline and indicators had to be developed retrospectively for the purposes of this Fitness Check.

3. How has the situation evolved over the evaluation period?

Consumer participation in digital markets

According to Eurostat, household consumption expenditures accounted for 51% of the EU's GDP in 2022, which highlights the continued importance of the role that EU consumers play in the internal market (compared to 50.2% in 2020 and 52.7% in 2015). According to the representative 2023 Consumer Conditions Scoreboard, which covered 27 000 consumers in the EU27, Iceland and Norway, **71% of consumers had purchased goods or services online in the past 12 months, which is a 23.2 percentage point increase compared to 2016.** Among those who made an online purchase, 61% bought from traders in their own country, whereas only 27% bought from another EU country and 20% from traders outside the EU. There continue to be large differences in the uptake of e-commerce by age: while more than 4 in 5 of those in the age groups 18-34 and 35-54 report they had bought online (81%), the proportion reduces to two thirds of those aged 55-64 (66%), and to half of those over the age of 64 (51%). Similar differences exist by education level - 51% of consumers whose highest education level was lower secondary education or below made purchases online, compared to 79% among respondents with some tertiary level education. A rural/urban divide in the use of online buying is also apparent. Around two thirds of those living in rural areas bought online in the last 12 months (67%), compared with almost three quarters of those living in large towns (74%).

According to the representative consumer survey for this Fitness Check, which covered 10 000 consumers from 10 Member States (DE, EE, ES, FR, IT, HU, PL, PT, RO, SE), **most consumers (83%) had made some form of online purchase or used an online product or service in the previous 12 months (i.e. in 2022-2023),** whilst 15% stated they had not. Those in the older age groups were the least likely to have made online purchases: 22% of those aged 65+ and 17% of those aged 56-65 stated they had not purchased or used any type of product or service online, which is higher compared to 8% of respondents in both the 18-25 and 26-35 year-old groups. Consumers who indicated trust in online businesses and websites were most likely to have made online purchases (95%). Responses also showed that the likelihood of consumers making an online purchase are proportionate to income levels, those on the highest income being more likely to have purchased or used online products or services, than those in the lower deciles: 75% of consumers on average in the lowest 3 income deciles had made this type of purchase, this compares to 90% on average across the top 3 deciles.

Consumer participation in the Digital Single Market is exemplified by the massive growth of digital markets. These rapid development pose challenges and opportunities for consumer rights, given that innovations in applying new technologies, business models, payment methods, use of consumer data, behavioural insights and design of user interfaces mean that **traders are often testing new territory and consumer law will have to be applied in novel contexts**.

This growth of digital markets has brought consumers several benefits, such as new types of digital services and technologies, an increase in supply, choice and the possibility of comparing offers, as well as savings in transport, shopping time and an overall reduction in the accessibility gap for purchasing goods and services (e.g. for persons with disabilities, access from rural areas). The COVID-19 pandemic pressed many traders to switch to online sales, highlighting the potential of digital technologies to increase the economic resilience of businesses, and

bringing with it various benefits.

During the evaluation period, the role of e-commerce (i.e. online sales) in the EU's GDP rose from 2.5% in 2017 to 4.37% in 2022, and is estimated towards 4.68% in 2023.[15] E-commerce Europe and Eurocommerce presented in their 2023 European E-commerce Report that the **B2C e-commerce turnover was EUR 975 billion in 2023, which shows a significant growth of 65% compared to the 2018 baseline data of EUR 591 billion**.[16] According to data from Statista, the B2C e-commerce market revenues grew by 85% between 2017 and 2023 from EUR 187.7 billion to EUR 347.3 billion.[17] The e-commerce market has evolved from a simple counterpart of bricks-and-mortar retail to a complex shopping ecosystem that involves access via multiple types of devices, varying store concepts and business models, and innovative arrangements and relationships between consumers, traders and intermediaries. Online sales are expected to make up an average of 30% of retail turnover by 2030.[18] Revenue in the European e-commerce market is projected to show an annual growth rate of 9.1%, resulting in a projected market volume of USD 977.4 billion by 2029. [19] Within the EU's single market, e-commerce turnover grew even despite the UK leaving the EU and the lifting of COVID-19 pandemic measures, which had increased levels of e-commercial activity in the 2020-2021 period. Reasons behind this growth largely lie with the increasing share (>90%) of populations accessing the internet, and easier access to digital devices, especially smartphones.[20]

Moreover, the EU's platform economy has grown exponentially from an estimated EUR 3 billion in 2016 to EUR 14 billion in annual revenues by 2020.[21] In 2023, it was estimated that Europe saw a growth of 24.8% in the value of the platform economy to a total value of USD 314.60 billion. According to research by the JRC, while examining the proportion of platforms with a local origin for each MS, fewer than 50% of all platforms operating in a given European country had a domestic origin, except Bulgaria and Slovakia.

The digital subscription economy also increased, with the average European household spending 130 EUR per month on subscriptions for an estimated market worth of EUR 350 billion, of which digital product and service subscriptions (e.g. software, music, video-on-demand and games) are valued collectively at EUR 30 billion.[22] The latter category is outstripping tangible goods subscriptions and expected to grow further, with young Europeans continuing to subscribe at a higher rate.[23] Overall, the digital subscription economy has tripled since 2017. According to a Deloitte study, the global digital subscription market is dominated by the US,[24] accounting for over half of the global market, followed by Europe (21% or EUR 78.6 billion) and China (14%), respectively.[25]

Digital advertising became the largest advertising channel globally in 2016. In 2021, traders spent EUR 46 billion on digital advertising in the EEA, which is more than the spending on all

[15] Lone, S., Luharuwala, A. and Weltevreden, J. 'European E-Commerce Report 2023', Amsterdam/Brussels: Amsterdam University of Applied Sciences, Centre for Market Insights, Ecommerce Europe and EuroCommerce & Wholesale, Amesterdam/Brussels, 2023.
[16] Ibid.
[17] 'eCommerce – EU-27', Statista Market Insights, May 2024.
[18] Lone, S. and Weltevreden, J. 'European E-Commerce Report 2022', Amsterdam/Brussels, Amsterdam University of Applied Sciences, Centre for Market Insights, Ecommerce Europe and EuroCommerce & Wholesale, Amesterdam/Brussels, 2022.
[19] 'eCommerce – Europe', Statista Market Insights, May 2024.
[20] Lone, S. and Weltevreden, J. 'European E-Commerce Report 2022', Amsterdam/Brussels, Amsterdam University of Applied Sciences, Centre for Market Insights, Ecommerce Europe and EuroCommerce & Wholesale, Amesterdam/Brussels, 2022.
[21] 'The EU's platform economy', Council of the European Union Infographics, March 2024.
[22] ING Economics Department, 2018. Now that we subscribe to music, are tools and toiletries next? Opportunities and challenges for tangible goods subscriptions, Sustainable transitions: circular economy.
[23] Ibid.
[24] 'Digital media: the subscription prescription', Deloitte.
[25] 'Market distribution of the digital subscription economy worldwide in 2020, by region', Statista.

other advertising channels combined.[26] The European digital advertising market reached an estimated EUR 86 billion in 2022.[27] The global digital advertising market is projected to grow by 6.87% (2024-2028) resulting in a market volume of USD 965.6 billion in 2028. The means through which digital advertising will be spent will also shift, with an increase to 70% of total ad spending that will be generated through mobile in 2028. The European digital advertising market is projected to grow by 6.0% (2024-2028) resulting in a market volume of EUR 148.7 billion in 2028. The size of the global market for AI in personalised marketing was valued at USD 1.18 billion in 2023 and is expected to increase in size by 27.1% in the 2023-2030 period.

The Fitness Check also examined various practices in specific B2C sectors, such as social media, gaming, entertainment services and online dating, which increased their market size over the evaluation period. In 2023, 84% of young people aged 16-29 years used social media networks[28] and globally, the average consumer spent 151 minutes on social media per day.[29] Compared with 2016, the global market value of influencer marketing on social media had increased by 700% to USD 14 billion in 2021.[30] According to a 2019 Eurobarometer survey, 48% of EU consumers stream music, 47% watch movies or TV shows and 27% play video games.[31] The European entertainment services market is estimated at EUR 91.4 billion for the audiovisual sector, EUR 23.5 billion for the video games sector and EUR 19.8 billion for news media.[32] The global online dating services market is estimated to be USD 7.9 billion in 2022, with up to 278 million consumers using them by 2024.[33]

The European video game market features 126.5 million players, with 41.5% of revenues coming from paid apps and in-app purchases in 2022.[34] In 2018, the European video game market was worth EUR 21 billion, with a 15% year-on-year growth rate. Revenue generated from loot boxes used in video games is expected to exceed USD 20 billion by 2025,[35] although specific figures for European markets are not available. For comparison, a call for evidence in the UK found that the UK loot box market was estimated to be worth EUR 812 million in 2019.

Consumer markets have changed and continue to evolve as a result of several technological developments, such as the growing use of AI, the increase in data-driven personalisation, connected products like virtual assistants, algorithmic contracting, the emergence of virtual worlds etc. Typical European households have circa 20 connected devices.[36] In 2022, 72% of internet users in the EU used Internet of Things (IoT) devices or systems: 64% used smart home entertainment solutions such as internet-connected TV, game consoles, home audio systems and smart speakers, 29% were wearing a smart watch or a similar wearable, 11% used smart meters for energy management in the home, 10% used smart home appliances such as robot vacuums, fridges, ovens and coffee machines, and nearly 10% used internet-connected home alarm systems and other safety and security solutions for their home.[37] Europe's IoT market was

[26] European Commission (2023), Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers.
[27] 'AdEx Benchmark 2022 Report', IAB Europe, July 2023.
[28] 'Digital skills - ICT usage in households and by individuals', Eurostat, 2023.
[29] Daily time spent on social networking by internet users worldwide from 2012 to 2023.
[30] 'The impact of influencers on advertising and consumer protection in the Single Market', EP study, 2022.
[31] 'Accessing Content Online, Cross-border Portability of Online Content Services and Intra-EU Calls', Eurobarometer, European Commission, 2019.
[32] 'The European Media Industry Outlook', European Commission, 2023.
[33] Number of dating service users worldwide from 2017 to 2027 by segment, Statista, 2020.
[34] 'All About Video Games, Culture – Creativity – Technology, European Key Facts 2022', Video Games Europe and European Games Developer Federation.
[35] 'Video Game Loot Boxes to Generate $20 Billion in Revenue by 2025', Juniper Research, March 2021.
[36] SWD from Impact assessment of radio equipment for activation of delegated acts on security of devices to improve data protection and privacy and protection from fraud, European Commission, 2020, based 'Final Report - Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment', Centre for Strategy & Evaluation Services and Tech4i2, April 2020.
[37] Eurostat, Digitalisation in Europe – 2024 Edition.

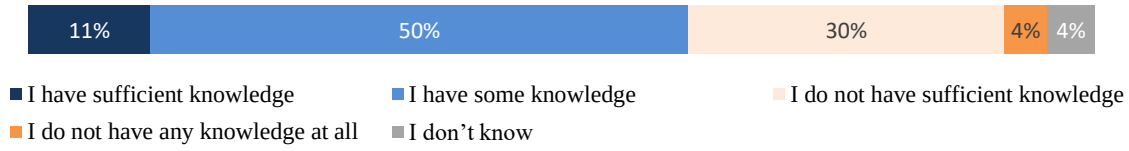
valued at approximately EUR 2 billion in 2021 and it is projected to reach EUR 11.5 billion by 2031. In 2021, the virtual and augmented reality industry in Europe was estimated at EUR 9.6 billion and forecasts estimate that by 2031, different consumer and business use cases in virtual worlds could contribute up to USD 3 trillion to the global GDP, for example in the areas of e-commerce, gaming, socialising and fitness. [38]

As explained further in the sections on effectiveness and efficiency, the above-mentioned increase in consumer engagement in digital markets can be attributed at least partly to the development of the EU consumer law acquis, including the three Directives.

Consumer awareness of their rights

In order to exercise their rights in case problems arise, consumers need to know that such rights exist and can be applied in the digital environment, as well as how to file complaints and resolve disputes. Over the evaluation period, the CCS showed that **knowledge of consumer rights remains insufficient**: in 2016 only 12.6% of consumers demonstrated high knowledge when tested about their rights (all answers correct), against 28% in 2023 (aware of at least three of the four rights tested)[39], with significant variations between countries. In terms of consumer confidence in their own knowledge, as shown in the 2023 representative consumer survey, only 11% of consumers stated that they had sufficient knowledge, 50% felt they had some knowledge and 30% not have enough knowledge.

Figure 1 – Consumer knowledge of their rights online[40]



Source: Consumer survey to support the Fitness Check

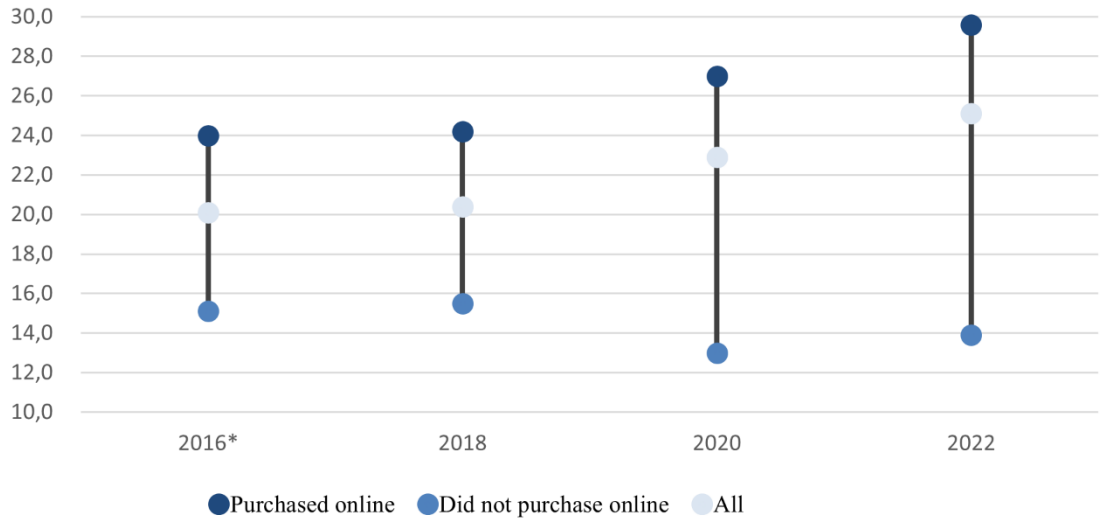
Several measures have been taken to address these concerns. For example, during the evaluation period, in 2019 the Commission carried out a consumer protection awareness-raising campaign called "You're right", which had a strong digital focus and targeted 18-35 year-old digital natives (i.e. consumers who grew up with the presence of digital technology or in the information age) who are active online shoppers. Notwithstanding this action and additional actions at national level, a lack of awareness of consumer rights continues to undermine the effectiveness of EU consumer law also in the digital environment and awareness-raising efforts may need to continue in the future.

Consumer complaints in the context of digital growth

Despite the growing importance of digital services and the benefits brought by technological advancements, consumer reports of problematic practices remained high over the evaluation period (24-30%), as shown by the Consumer Conditions Scoreboard graph below.

[38] EP study (2023) Metaverse, p. 31.
[39] Measured in terms of the percentage of consumers responding correctly to questions about their rights; without distinguishing between the online and offline environment.
[40] "In general, how would you rate your knowledge about consumer rights that may apply to you in the digital environment (e.g. when purchasing digital content and services, or when using digital platforms such as social media)?" (n=10,000)

Figure 2 – Consumer Conditions Survey: % of consumers who experienced a problem when buying goods or services in their home country by online shopping status (2016-2022), EU27[41]



Source: Consumer Conditions Scoreboards 2017-2023, based on data collected in 2016-2022

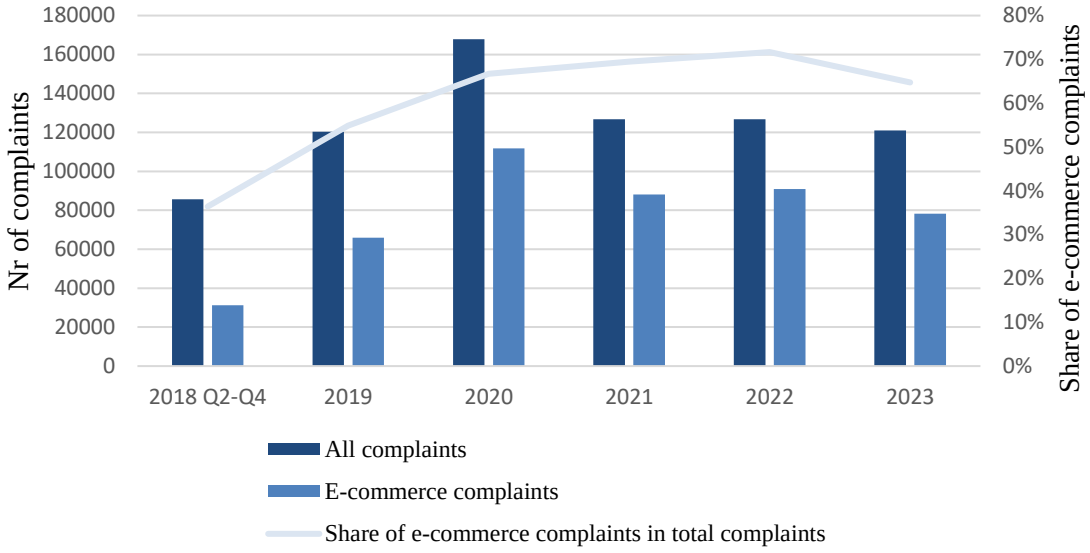
The overall number of complaints remains high, especially for online purchases. The representative 2023 CCS (based on 2022 data) found that approximately **30% of consumers making online purchases experienced a problem** for which they felt there was a legitimate reason to complain, which is an increase of 6 percentage points compared to 2016. **Those who purchased online were twice as likely to have experienced problems than those who did not purchase online.** Younger consumers aged 18-34 were more likely to have experienced a problem than others. The most serious problems were reported to a **similar extent with traders in the consumers' own Member State, in another EU Member State or in non-EU/EEA countries**. In principle, in order to consider the three Directives to be effective, there should be a reduction in the number of problems encountered by consumers, reflected by a lower number of complaints (towards the Commission's target of lowering the overall share of consumers experiencing problems to 15% in 2027 in both online and offline scenarios). As shown by the data, this target has been reached for offline purchases, but not for online purchases. However, a higher number of complaints can also be indicative of factors such as the increased awareness of consumer rights and the improved availability of complaint-handling mechanisms, which are positive from the consumer policy perspective. Therefore, it should be noted that any analysis of consumer complaints and detriment should be based on a multitude of complementary sources, including opinion-based evidence.

As a complementary source of data in addition to the figures from the CCS, more granular data on cross-border consumer complaints can be found from the European Consumer Centres (ECC) Network. The graph below gives an overview of how the **number of cross-border e-commerce related complaints** has evolved between the period Q2 2018 and 2023.[42]

[41] Q: "In the past 12 months, have you experienced any problem when buying or using any goods or services in your country where you thought you had a legitimate cause for complaint?" (n= approx. 27 000). *Results for 2016 are estimated, to account for changes to the weighting of survey results in 2018.

[42] E-commerce complaints are complaints resulting from four categories of selling methods: internet auctions, internet platforms, e-commerce and intermediaries other than booking.

Figure 3 - European Consumer Centres Network overview of the share of cross-border e-commerce consumer complaints in the overall number of consumer complaints (2018-2022)



Source: ECC-Net data

The overall number of cross-border complaints and the number of e-commerce complaints remains high. The figure below shows that the number of e-commerce complaints followed the same pattern as the number of overall complaints, increasing and decreasing in the same years. However, there has also been a noticeable increase in the share of e-commerce complaints in relation to the overall number of complaints in the period 2018-2022. The share of e-commerce complaints was 36% in 2018 but steadily increased to 55% in 2019, 67% in 2020, 69% in 2021 and 72% in 2022, after which it decreased to 65% in 2023. The steep increase in the number of complaints in 2020 was primarily a result of the COVID-19 pandemic. The overall increase in e-commerce complaints can be partially explained by consumers buying more online and buying more from traders from other EU/EEA and non-EU/EEA countries. However, it is also indicative of continuous consumer protection issues present in cross-border e-commerce. It is not possible to say with certainty what caused the slight decrease in the number of total complaints and e-commerce complaints in 2023, but it may be a result of rising costs of living, which has led to a decrease in cross-border consumer spending. Out of a total of 466,290 complaints in the period 2018-2023, the Member States with the highest number of e-commerce complaints were Belgium (56,086 complaints), followed by France (49,836 complaints) and Austria (35,758 complaints), whereas the lowest number of complaints originate from Malta (2675), Cyprus (2578) and Croatia (2506). Several factors could have an impact on why consumers in some countries complain more frequently to ECCs compared to those in other countries, such as differences in the national legal framework, consumer rights awareness levels and access to complaint mechanisms.

Notably, the above overviews of complaints[43] are likely to underestimate the scale of the problem, since the 2023 CCS showed that most consumers who take action after experiencing a problem complain directly to the trader (81%), whereas only a minority will bring the matter to a consumer organisation or European Consumer Centre (11%), ADR body (6%) or to court (3%). Moreover, many consumers do not take any action at all due to a variety of reasons, such as thinking it would take too long, the sums involved were too small, unlikeliness of getting a satisfactory solution to the problem, avoiding confrontation etc.

However, for the purposes of this Fitness Check, **the number of consumer complaints must be put into context and interpreted more meaningfully by neutralising the effect of digital market growth and e-commerce uptake, as well as accounting for inflation**. For example, the share of consumers buying online has risen from 54% in 2017 to 70% in 2023. The e-commerce uptake increased sharply during the COVID period due to physical shopping limitations. In view of this increase, especially between 2021 and 2023, **there have been fewer consumer complaints than could have been expected in view of the annual e-commerce growth rate**. In order to assess the overall evolution of consumer detriment related to these complaints and to quantify the harm, additional analysis was carried out (see next sub-section on financial detriment).

Scale of specific problems

In addition to outlining the general trends related to problems that consumers experience in the digital environment and the parallel growth of digital markets, the Fitness Check examined specific problematic practices that make up a significant portion of the consumer complaints and fall under the scope of EU consumer law. There is **additional analysis of the specific problematic practices identified in Annex VI** concerning the nature and extent of the problems, including how the current EU legal framework tackles them and the possible solutions emerging from stakeholder consultations.

A **distinction must be made between problematic practices and the related technologies or business models, which are not problematic as such**. For example, misleading influencer marketing is presented as a problem, but social media as an advertising channel is recognised as a very positive development, which helps consumers to find, research and buy new products and services more easily. Likewise, personalisation of advertising and recommendations is presented as a positive development, which can help to direct consumers to more relevant purchases and content. However, the misuse of consumer vulnerabilities or sensitive data for personalisation purposes is presented as a problem. The problematic practices assessed in the Fitness Check involve behaviour that would be likely to be non-compliant with consumer law (e.g. unfair, misleading or aggressive practices, unfair contract terms), whereas the potential benefits of legitimate tech-uses are duly recognised.

[43] Additional insights about the evolution of consumer complaints can be found from the Online Dispute Resolution (ODR) platform, which allows EU consumers to contact traders to resolve disputes about goods or services bought online from traders based in the EU, Norway, Iceland or Liechtenstein. The overall number of complaints per year has remained high, although the use of the ODR platform decreased over time: 32 559 (2017), 44 979 (2018), 31 694 (2019), 17 461 (2020), 13 246 (2021) and 17 012 (2022). The most complained about sectors included airlines (19.74%), clothing and footwear (9.36%), ICT goods (6.45%), electronic goods (4.56%), and holiday accommodation (4.05%). For an explanation of the state of play of the ODR platform, see the Annex 6 of the Impact assessment report for the Proposal for a Directive amending Directive 2013/11/EU on alternative dispute resolution for consumer disputes, as well as Directives (EU) 2015/2302, (EU) 2019/2161 and (EU) 2020/1828. The decreasing number of complaints is not an indicator that consumers are facing fewer problems, but rather points to broader issues with the ODR platform, which are further analysed in the documents accompanying the Commission's 2023 proposal to repeal the ODR Regulation. For example, 80-85% of complaints went unanswered by traders on the platform and only about of 1% of the complaints resulted in an ADR outcome.

Remarks on methodology regarding the scale and development of problems

The scale and development of problems has been estimated primarily using representative survey data (e.g. CCS, consumer survey, Eurostat) on the incidence of problems encountered in the digital environment by consumers and the perceived detriment levels. This has then been contrasted by the change in market size and structure during the evaluation period, as it is important to contextualise the figures. For instance, ***a problem may have remained of the same scale in frequency as a percentage of consumers affected, but the market may have doubled in size within 5 years leading to a doubling of detriment****.*

To complement the survey-based quantification of overall detriment across digital markets, desk research was undertaken to identify and review relevant secondary literature addressing consumer detriment across specific thematic problematic practices. Where robust survey data was identified from earlier studies, this provided a proxy for establishing the baseline regarding the problem's scale in around the 2017 period, with a view to analysing problematic practices and determining how far these evolved between the baseline and current situation. Where no comparable evidence was found, this was clearly indicated.

The main methodological challenges in this context include the very ***wide-ranging scope of problematic practices covered*** *in this Fitness Check, covering nearly all B2C sectors, and the fact that* ***some problematic practices are relatively new*** *- whilst studies have been undertaken in particular in the last three years, there is a lack of literature on the extent of the problem dating back to the 2017 baseline (e.g. dark patterns, loot boxes). Conversely, other topics, such as subscription traps, were covered in earlier studies, thereby providing some baseline data, although caution should nevertheless be exercised in directly comparing the survey results from different studies, given different survey cohorts, differences in question phrasing etc.*

Overall, the data collected from desk research and consultation activities, including stakeholder perceptions in response to the targeted survey, show that **there has been an increase in the frequency of different problematic practices during the evaluation period, which is consistent with the growth of digital markets**. It is also considered likely that the frequency of these problems will continue to increase in the future (e.g. as markets grow and new technologies become available to more traders), which could undermine consumer trust in the digital economy. The scale of specific problems and their increase during the evaluation period varies. For example, while problems with dark patterns and commercial personalisation affect nearly all consumers that use the internet, **some problems are more 'niche' and affect particular consumer segments**, such as 27-53% of consumers that play video games, of which a smaller percentage of consumers frequently purchase in-game virtual items, and of which an even smaller percentage buy loot boxes. However, even for problems that affect only a specific cohort of consumers among the total population, the detriment at stake can be significant (e.g. the loot box market is estimated as being worth billions of EUR).

Five categories grouping the most commonly reported problematic practices that fall within the scope of the three Directives are briefly summarised in the following table, with **key data on the scale of the problems highlighted**. The selection of these issues entails a prioritisation based on the relative scale of the problems common across the EU27, whereas the corpus of practices that are problematic from a consumer protection perspective is much wider.

Category	Figures from the data collection and consultations
Dark patterns	Dark patterns are commercial practices deployed through the structure, design or functionalities of digital interfaces or system architecture that can influence consumers to take decisions they would not have taken otherwise, e.g. presenting choices in a non-neutral manner, using fake countdown timers to create urgency, using emotional manipulation to make consumers second-guess their indicated choice, phrasing questions using double negatives, misleading consent options in cookie banners. Although traders' attempts to influence consumer decision-making is not a new phenomenon, **concerns have intensified about the increased**

effectiveness and scale of such practices as well as the potential for personalised persuasion based on behavioural data.

While there are no existing baseline figures from 2017 for each type of dark pattern, there have been numerous enforcement actions in the past five years against various misleading online practices (e.g. drip pricing, subscriptions traps, hidden information[44]), which were not previously labelled as 'dark patterns' but simply as consumer law breaches. The problem with the prevalence of dark patterns has arguably become worse, as illustrated by the sharp increase of policy attention and regulatory or enforcement action from European and other authorities globally in the last three years (e.g. US, UK, South Korea, India; OECD Committee on Consumer Policy). In the targeted survey, 61% of respondents perceived an increase of the deployment of dark patterns during the evaluation period. The Commission's 2022 dark patterns study showed that **97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern**, with the most common ones involving hiding information, creating false hierarchies in choice architectures, repeatedly making the same request, difficult cancellations and forced registrations. The 2022 CPC sweep by EU consumer authorities found that nearly **40% of online retail shops contained at least one dark pattern**, specifically fake countdown timers, hidden information and false hierarchies in choice architectures. The 2024 International Consumer Protection and Enforcement Network (ICPEN) and Global Privacy Enforcement Network (GPEN) sweep of the websites/apps of 642 traders found that 75,7% of them deployed at least one dark pattern, and 66,8% of them employed two or more dark patterns. Sneaking practices (e.g. inability of the consumer to turn off auto-renewal of subscription service) and interface interference (e.g. making a subscription that is advantageous to the trader more prominent) were encountered especially frequently.

Concerning evidence of current problems, in the representative consumer survey, 40% reported experiencing a situation where the design or language used on a website/app was confusing, which made the consumer uncertain about what they were signing up for, or about which rights and obligations they had. 66% saw claims that a product was low in stock or high in demand (e.g. that many other consumers are currently looking at the same product) and 61% saw claims that a product was available only for a limited time, without the ability to know if these claims are truthful. 32% reported paying more than they planned to because during the purchasing process the final price changed to a price higher than the one advertised initially. 48% of consumers, especially the young, were pressured with repeated requests to make a decision, e.g. to get a premium account, offering special discounts, asking to buy a recommended product. After indicating their choice or declining a choice offered, 42% received messages that made them doubt their decision, e.g. asking questions like 'are you really sure you do not want a discount?'. 37% recognised a situation where important information was visually obscured

[44] For example, in 2018, the CPC network screened 560 e-commerce sites offering various goods and services, finding problems on 211 of the sites concerning the final price at payment being higher than the initial price offered and 39% of those traders did not include proper information on unavoidable extra fees on delivery, payment methods, booking fees and other similar surcharges.

	or ordered in a way to promote an option that did not seem to be in their interest. 37% encountered preselected options that were in favour of the company but changing those options was difficult. 42% experienced a situation where making a choice led to a different result than they would normally expect, e.g. clicking an unsubscribe button led to a page describing the benefits of that service that you would lose. Dark patterns can affect a wide range of transactional decisions and many of them have been empirically proven to appreciably impair the consumers' ability to take an informed decision. In the public consultation, 89% of consumers reported being confused by dark patterns in website/app design and 76% felt pressured to buy something due to the language or design that was used. The behavioural experiments in the Commission's 2022 dark patterns study showed that when exposed to dark patterns the probability of making a choice that was inconsistent with the consumers' preferences increased – the average figure of making inconsistent choices arose to 51% for vulnerable consumers and 47% for average consumers, with older consumers and those with lower education levels being more impacted.
Addictive design and gaming	As consumers navigate the 'attention economy'[45], concerns have increased regarding specific interface designs and functionalities that could induce digital addiction. It is generally in the traders' economic interest to design their products in a manner that increases the amount of time, money and engagement that consumers spend, especially those traders whose business model relies on the processing of consumer data. However, the **addictive use of digital products and services carries the risk of economic, physical and mental harm**, including, but not confined to, vulnerable consumers such as children. While most of the addictive design features already existed in 2017, both the **market size and consumer use of products like social media and video games in the EU have increased over the evaluation period**. Furthermore, algorithmic recommendations and other data-driven practices improved in their efficacy and persuasiveness as more consumer data was gathered through the years. The EP's 2023 resolution on addictive design of online services highlighted the negative impacts that addictive design could have on consumers, including mental health problems, especially for younger consumers.[46] In the representative consumer survey, **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**. In the public consultation, 33% of consumers reported spending too much time or money using certain websites or apps for hours. Concerns have also arisen with specific products such as video games that increasingly involve the sale of virtual items, including uncertainty-based rewards (e.g. loot boxes), and the use intermediate in-app virtual

[45] The term attention economy refers to the range of economic activities based on people's attention being treated as a scarce and highly desirable resource to be captured and maintained.

[46] Lopez-Fernandez, O. and Kuss, D., 'Harmful Internet Use Part I: Internet addiction and problematic use', European Parliament Research Service - EPRS, STOA, January 2019, p. 51.

	currencies, which could distort the real value of the transaction for consumers and encourage them to spend more than they intended. Furthermore, these practices are often accompanied by opaque offer and pricing techniques. The proliferation of commercial communications in gaming environments raises different concerns that are currently not expressly addressed by any EU law. Over the evaluation period, there has been an **increase in the use of in-game purchases and virtual items like loot boxes**. In 2018, 74% of the video game turnover came from app and online revenues, compared to 83% in 2022.[47] Loot boxes were much less widespread in 2017, compared to 2023. Concerns have also been amplified due to the widely increased accessibility of such apps to minors given the ubiquity in the availability of smartphones and tablets. The targeted stakeholder survey showed that 68% of respondents considered the use of loot boxes and addiction-inducing features to have increased over the evaluation period. In the representative consumer survey, 29% of consumers had experienced a situation where the real price of a virtual item was not clear because it was only indicated in the app's virtual currency.
Personalisation	As a cross-cutting issue, concerns about the use of consumers' personal data have increasingly undermined consumer trust over the evaluation period. Personalisation practices in the B2C context can take the form of behavioural advertising, search result ranking, recommendations, prices etc., which can offer many benefits for consumers. However, the **2023 CCS found that 70% of consumers are concerned about how their personal data is used and shared, which amounts to a 21 percentage point increase compared to 2018**. Targeted advertising was already prevalent in 2017 and continues to be used extensively, as digital advertising has become the largest advertising channel globally. The targeted stakeholder survey showed that 53% of respondents perceived personalised pricing to have increased in frequency over the evaluation period, although these practices are difficult to detect. Data collection in policy discourse and research has become more frequent after the entry into application of the GDPR in 2018. Furthermore, the 2023 CCS also found that consumers continue to be concerned about the processes concerning the collection of personal data and profiling (66%), installation of cookies (57%), negative effects on their trust in e-commerce (38%), seeing only a limited selection of ads and not the best offers (38%), inability to opt-out/refuse (37%) and inability to distinguish between information and advertising (35%). The representative consumer survey found that 41% of consumers had experienced a situation where the design or language of the website/app made it difficult to understand how their personal data would be used, and **37% of consumers had the impression that the company had knowledge about their vulnerabilities and used it for commercial purposes**. In the public consultation, 74% of consumers thought their personal data was misused or used unfairly to personalise commercial offers in the preceding 12 months. BEUC's representative 2023 survey showed that the **majority of consumers do not consider personal data**

[47] Video Games Europe – key facts from 2022 and 2019 reports.

	analysis and monetisation to be fair (60%) and they do not feel fully in control of the decisions they make or the content they are shown online – consumers reported feeling unsafe (60%), manipulated (55%) or suspected that their rights were violated (46%), yet less than half of consumers considered filing a complaint and only 22% felt satisfied by how authorities are protecting them against unfair practices. These concerns were heightened in case of personal data about vulnerable consumers who are more at risk, in particular children.
Social media	With the increasing importance of social media for consumer transactions, reports of problematic practices have become more prominent. While direct purchasing possibilities through social media platforms (e.g. 'buy' buttons, shopping carts) have not yet been widely rolled out in European markets, social media is helping consumers to discover, research and buy new products and services. However, non-compliance with the requirement to clearly disclose commercial communications is widespread. While there are no existing baseline figures from 2017 regarding problematic practices by influencers (e.g. questions on influencers were included in the CCS since 2022), it is estimated that the **size of the market has increased over 700% since 2016, which can be presumed to bring with it an increase of non-compliance**, especially since influencers may not have the same level of legal knowledge as professional traders. In the targeted survey, 51% of respondents perceived an increase in the lack of transparency concerning paid promotions by influencers during the evaluation period.[48] The 2024 CPC sweep by EU consumer authorities found that **just 20% of influencers systematically indicated the commercial nature of the content shared**. In the representative consumer survey, 45% consumers, especially younger age groups, noticed that the content they were viewing seemed to be a paid promotion or advertisement, but the website/app did not make this clear. In the public consultation, 74% of consumers reported a lack of transparency about the paid promotions of products by social media influencers and 55% of respondents reported the same in the representative 2023 CCS. Concerns arise not only with hidden marketing, but also with the possibly problematic content of the advertising, such as specific products promoted or sold through influencers. BEUC's representative 2023 survey found that **44% of consumers have seen influencers promoting scams or dangerous products**. The exposure of children to aggressive marketing of unhealthy food and beverages, alcohol or vaping, is also a point of increasing concern. Furthermore, it is not sufficiently clear for market participants which degree of responsibility should be exercised by the various traders involved, such as the influencer, brand and online platform.
Digital contracts	In the context of the exponential growth of the digital subscription economy and the trend towards 'freemium'[49] business models, consumer have increasingly encountered problems with their digital contracts.

[48] 'Influencer marketing market size worldwide from 2016 to 2024', Statista, February 2024.
[49] The term freemium refers to a business model in which the consumer is offered basic or limited features at no cost but charges a premium for additional, more advanced features.

While there are no existing baseline figures from 2017 for each issue related to digital contracts, the subscription economy market has tripled since 2017[50] and figures from previous studies show that **problems with difficult cancellations and subscription traps have increased**. For example, in 2017, 7% of consumers reported experiencing problems with subscriptions[51], compared to 14% in 2020[52] and much larger figures identified in this Fitness Check (see granular survey data below; up to 60 percentage point increase from 2017 to 2023). In the representative consumer survey, **40% considered that the design of the website/app made cancelling the subscription very difficult**. The sweep in the framework of the supporting study showed that traders provide clear information about the 14-day right of withdrawal in only 54% of cases and the procedure for cancellations beyond 14 days was only fairly clear in 34.7% of cases. In the representative 2023 CCS, 23% of consumers reported difficulties with cancelling a contract that they had concluded online. In the public consultation, 69% of consumers found it technically difficult to cancel their contracts, 55% experienced deliberate avoidance of contract cancellation by the trader and 34% were only able to cancel their subscriptions after a longer time period (e.g. a year), despite being charged monthly.

Auto-renewals can be convenient and beneficial for consumers, provided the consumers are aware of them. In the representative consumer survey, **29% of consumers reported often having their free trial automatically extended into a paid subscription**. Consumers also indicated that they continued paying for a digital subscription that they had stopped using some time ago but forgot to cancel (18% encountered this often, 19% sometimes). 62% of consumers in the public consultation experienced automatic renewals of inactive subscriptions without reminders.

Consumers have limited bargaining power when entering into contracts in the digital environment – in general, they can either take it or leave it. The detection of unfair contract terms presumes that consumers are able to familiarise themselves with the contract terms in the first place, but most consumers never choose to do so. In the representative consumer survey, **only 36% of consumers indicated that they read the Terms & Conditions always or often**, with a further 23% indicating they do this sometimes. The **prevalence of unfair contract terms has increased** over the evaluation period. According to the CCS, in 2017, 9.8% of consumers encountered unfair contract terms, compared to 22% in 2023, without however distinguishing between contract terms in offline vs online environments. Additional sources, such as the 2017-2018 CPC sweep into the telecommunication and digital services sector showed that 31.9% of websites had problematic T&Cs and academic literature highlights that during the reference period of 2016-2017, unfair contract terms were

[50] In Europe, Business Wire noted the subscription economy had growth greater than in the USA, with annual growth rates often exceeding 25% in recent years. In 2023, the subscription economy in Europe had turnover of approximately EUR 199.4 billion.

[51] ECC-Net, Subscription traps in Europe: Study into public experiences of subscription traps in six countries (2017).

[52] 'Survey on "Scams and Fraud Experienced by Consumers" – Final Report', European Commission, January 2020.

	already prevalent in the T&Cs of online platforms.[53] Concerning evidence of current problem, in the public consultation for this Fitness Check, 62% of consumers perceived a contract term to be unfair when buying a digital service or digital content, but nevertheless had to agree to it. As a result of the unfair terms, in the representative consumer survey, 21% indicated they had suffered financial harm because they did not know all the conditions that applied to their contract, or lost time because it was not clear where to find the T&Cs (35%), or had their privacy harmed because they unintentionally agreed to share more personal data than intended (29%).

Financial consumer detriment quantified

When traders engage in problematic practices and do not comply with the three Directives, whether intentionally or negligently, **consumers can suffer detriment**. In the digital context, consumer detriment could be defined as a situation in which **consumers experience negative outcomes when taking transactional decisions regarding different products and services online** (as opposed to structural consumer detriment attributable to market failure or regulatory failure). Detriment can also be viewed as unrealised benefits that were meant to result from the proper application of the Directives. Indicators that can be used to measure consumer detriment include the volume of complaints, levels of consumer (dis)satisfaction based on survey data and, in case the consumer took action to solve the problem, perceptions of the adequateness of the redress. Detriment can take the form of financial harm, including direct financial costs, and non-financial harms, such as mental health harms, time loss, annoyance, disappointment, and broader harms, such as different degrees of negative environmental impacts, which could ultimately influence consumer well-being. This Fitness Check measured **revealed personal consumer detriment**, which includes negative outcomes for individual consumers which they become aware of following the purchase or use of a product or service, measured relative to what would reasonably have been expected, given the type of transaction. In addition to qualitative data from surveys, it was possible to quantify the amount of pre-redress and post-redress financial detriment based on quantitative data obtained from the representative consumer survey.

Consumer complaints are a useful indicator regarding the **incidence of consumer detriment**, i.e. the proportion of consumers who experienced a problem in a given market in the last 12 months. As highlighted above, there has been an **increase of consumer complaints about problems online** over the evaluation period when comparing the representative figures of the CCS from 24% in 2016 to 30% in 2023. However, it was also noted that when taking into account the exponential growth of digital markets, the number of complaints is lower than what could have been expected. In order to better understand the **magnitude of revealed personal consumer detriment**, more granular data about detriment was collected in the representative consumer survey for this Fitness Check.

Importantly, the consumer survey arrived at an overall consumer complaint figure (27%) which is very close to the 2023 CCS figure (30%), thereby validating the assumption that, currently, **approximately one third of consumers face problems online**. When comparing this figure to quantitative data obtained from market sweeps, these figures are likely to be conservative and underestimate of the scale of the problem, since consumers may not be aware of the fact that they have been subjected to an unfair practice, especially if the issue does not concern the

[53] Micklitz HW, Pałka P, Panagis Y, 'The empire strikes back: digital control of unfair terms of online services', 2017, 40(3) J Consum Policy 367, 368; M. Lippi et al., 'Automated Detection of Unfair Clauses in Online Consumer Contracts', 2017, Legal Knowledge and Information Systems 145, 147.

purchase of physical goods (e.g. highly prevalent dark patterns such as misleading choice presentations in cookie banners may annoy consumers, but they might not realise that such practices are illegal, given their lack of awareness of their rights and the ubiquity of such practices). Similarly to the CCS, the consumer survey also validated the finding that the **highest level of detriment is amongst younger age groups** – problems were faced by 43% of those aged 18-25 and 38% of those aged 26-35, compared to 19% of those aged 56-65 and 16% of those aged 65+. Other notable differences in responses concerned the percentage of consumers who **engage in gambling activities** daily (48% faced problems, in comparison to 20% of those who never engage in gambling activities) and consumers whose daily activities are **severely limited due to a health problem** (42% faced problems, in comparison to 21% of those who have no health-related limitations).

Concerning **differences between product groups**, it is notable that 58% of consumer problems were related to purchasing physical goods online, while 33% of problems occurred with digital content or services. Concerning the **geographic location of the trader** with whom the problems were experienced, 46% were in the consumer's own Member State, whereas 27% were from another Member State and 18% from a non-EU country. Concerning the **duration of the problems** experienced, 43% of the problems did not last more than a week, whereas 31% lasted from one to week to a month. In terms of time spent seeking a solution, 62% reported that the amount of time lost did not exceed 4 hours. Overall, there were no significant differences between the scale of the problems reported by consumers from different Member States. National differences are further discussed in section 4.1.1.1 on 'effectiveness'.

The representative consumer survey was used to collect quantitative data about the financial detriment suffered by consumers as a result of the problems experienced. When presenting the figures, median numbers are used – the difference between the average and the median reflects the high variation in the costs experienced by consumers as consumer detriment. The median is less affected by outliers and skewed data than the mean and is usually the preferred measure of central tendency when the distribution is not symmetrical. The survey results show that **41% of consumers ended up over-paying or experiencing extra charges as a result of a problem** (median amount estimated at EUR 35). The median costs to consumers of repairs or replacement were estimated at EUR 30, the costs of dispute resolution or court proceedings were estimated at EUR 40, the costs of experts' advice were EUR 40 for those that sought advice. There were other additional costs such as phone call, postage and travel costs being reported, estimated at EUR 20. As a result of their dispute resolution efforts, consumers received EUR 50 of compensation. To calculate the overall amount of detriment, two values can be presented: a cost of detriment, pre-redress, that includes extra charges and costs of repairs estimated at EUR 65, and a cost of detriment, post-redress, that includes all costs (e.g. costs of dispute resolution and expert advice but also the reimbursement) estimated at EUR 115.

Table 3 – Quantification of the amount of individual financial consumer detriment suffered as a result of problematic practices in the digital environment in EUR

	Average (EUR)	**Median (EUR)**
Price paid for products	245	50
1. Extra charges as result of problem	137	35
2. Costs of repairs or replacement at your own expense	161	30

3. Costs of dispute resolution	214	40
4. Costs of experts advice	208	40
5. Extra costs	159	20
6. Reimbursement	251	50
Total costs of detriment (1+2) ***pre-redress***	298	**65**
Total costs of detriment (1+2+3+4+5 -6) ***post-redress***	628	**115**

Source: Consumer survey to support the Fitness Check

In order to extrapolate to the EU level, estimate the pre- and post-redress financial detriment at different times over the evaluation period and establish a baseline, the following formula was applied:

$$Financial\ Detriment_{year} = Total\ number\ of\ consumers\ \times$$
$$Percentage\ of\ all\ consumers\ with\ last\ internet\ online\ purchase\ in\ the\ last\ 3\ months_{year}\ \times$$
$$Complaint's\ incidence\ rate_{year}\ \times Individual\ Consumer\ Detriment_{year}$$

The various data points used for these calculations come from Eurostat and the Consumer Conditions Survey (CCS), with the latter being conducted on a biennial basis, therefore estimates can only be provided for every two years. The table below applies the formula to see how the detriment experienced by consumers who purchase online evolved over the evaluation period. For the purposes of the calculations, the number of consumers in the EU is estimated at approximately 440 million.

Table 4 - Extrapolation to the EU27 of financial consumer detriment suffered as a result of problematic practices in the digital environment over the evaluation period

European Union - 27 countries	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Percentage of all individuals with last internet online purchase in the last 3 months[54]	40.7%	43.7%	45.8%	49.0%	53.8%	56.9%	56.0%	40.7%
Complaint's incidence rate[55]	24.0%[56]		24.2%		27.0%		29.6%	
Inflation[57]		1.6%	1.8%	1.4%	0.7%	2.9%	9.2%	
Total cost of detriment pre-redress per problem experienced, in EUR, median[58]	52	52	53	54	54	56	61	65
Total cost of detriment post-redress per problem experienced, in EUR, median[59]	91	93	94	96	96	99	108	115
Pre-redress financial detriment estimate, total in billion EUR	**2.2**		**2.6**		**3.5**		**4.5**	
Post-redress financial detriment estimate, total in billion EUR	**3.9**		**4.6**		**6.1**		**7.9**	

Source: DG JUST, estimations based on Eurostat and CCS data

Overall, as shown in the table, **there has been an increase of consumer detriment over the evaluation period, even after taking into account inflation and e-commerce growth**. The post-redress financial detriment stood at **EUR 3.9 billion in 2016** before the evaluation period and is currently estimated at **EUR 7.9 billion** (based on the latest available 2022 data). For example, this allows to calculate that the consumer detriment amounts to 8 permille of e-commerce turnover in 2023, up from 6 permille in 2017, whereas business compliance costs (see section 4.1.3.1) related to the Directives amounts to 0.7 permille of the overall turnover in 2023. Overall, these numbers indicate that while there has been rapid growth in digital markets, which brings with it an increase in consumer benefits, there has also been a rapid growth in the consumer detriment. On the other hand, although approximately a third of consumers have experienced problems, the detriment relative to the overall turnover is modest. Until now, the detriment has not been severe enough to hinder consumers from using digital services or buying online, but there is a considerable risk that the persistence of problematic commercial practices

[54] 'Internet purchases by individuals (until 2019)' and 'Internet purchases by individuals (2020 onwards)' Eurostat, March 2024.
[55] Consumer Conditions Survey, Q15. In the past 12 months, have you experienced any problem when buying or using any goods or services in your country where you thought you had a legitimate cause for complaint? Yes 'Total of those that purchased online in the last 12 months' (%).
[56] Results for 2016 are estimated to account for changes to the weighting of survey results introduced in 2018.
[57] 'HICP - annual data (average index and rate of change' Eurostat, May 2024.
[58] Consumer survey to support the Fitness Check, figures until 2023 are deflated using the harmonised index of consumer prices (HICP).
[59] Consumer survey to support the Fitness Check, figures until 2023 are deflated using the HICP.

may undermine consumer trust in the future. This relativisation does not neglect the problems identified but puts them into perspective.

It should be noted that while the consumer detriment figure may serve as a **useful benchmark to provide an order of magnitude, it is likely to underestimate the total financial detriment to consumers**, since detriment can vary significantly depending on markets, segments and types of problems experienced, **and it does not tackle time loss or the costs of non-financial detriment (e.g. mental harm)**. Furthermore, **consumer detriment can be 'unrevealed' or hidden** in situations where a consumer has experienced detriment but remains unaware that it has occurred (e.g. overpaying for a product due to a dark pattern or hidden advertising by a social media influencer). Moreover, many consumers that experience problems do not make complaints or take any action to seek redress, which reduces the availability of relevant detriment data.

Additional sources of comparable data were sought in order to **triangulate and verify** the results.[60] In particular, the earlier Commission's 2017 consumer detriment study supporting the 2017 Fitness Check and the 2018 Impact Assessment for the Modernisation Directive can be compared with these figures. However, several caveats and methodological differences must be considered. On the one hand, the scope of the 2017 figure was broader – it covered both online and offline environments, as well as obligations going beyond these three Directives. On the other hand, the scope was smaller – it covered six markets (mobile telephone services; clothing, footwear and bags; train services; large household appliances; electricity services; and loans, credit and credit cards) and 4 countries (FR, IT, PL and the UK), whereas the consumer survey for this Fitness Check covered all relevant products and services in the B2C digital markets and in 10 Member States. Furthermore, pre-redress financial detriment estimates from the two studies are not comparable as several extra costs related to solving the consumer's problem are not included in the pre-redress costs in the 2017 study but in post-redress costs. However, the post-redress financial detriment to consumers can be compared. The 2017 Commission's consumer detriment study provides two estimates for detriment because it included both an online survey and face to face interviews. The incidence rate of problems was lower in the face-to-face interviews. The online panel estimate is therefore chosen for the comparison of the total cost of detriment to consumers as it is the same survey mode that was used in the consumer survey in 2023. The online panel estimated that consumers suffered post-redress financial detriment of EUR 33.3 billion in 2017, for online and offline problems. There is corroborative evidence[61] that in 2017, the share of e-commerce in the retail sector stood at

[60] Additional data sources were sought to compare the incidence of detriment and to estimate the order of magnitude for post-redress financial detriment in the digital environment. For example, the 2015 Commission Impact Assessment accompanying the proposal for a Digital Content Directive showed that the lack of specific consumer rights for digital content (i.e. music, anti-virus software, video games and cloud storage services) caused consumer detriment, which was estimated between EUR 9-11 billion in the EU. This estimate is very close to the figure in this Fitness Check, confirming the validity of the order of magnitude of the digital-specific detriment estimate. As an additional example, the 2020 Commission study on scams and fraud estimated that consumers suffer EUR 24 billion of financial losses due to such problems over a two-year period. This figure included specific detriment directly relevant for the topic of dark patterns and digital subscriptions covered in this Fitness Check: the study found that 8% of consumers had fallen victim to a subscription trap (i.e. being tricked into a monthly subscription after having purchased a free or relatively cheap product or service) and the estimated financial cost relating to such online subscriptions was approximately EUR 1.92 billion across a two-year period. This magnitude of this estimate is consistent with the figure in this Fitness Check, which is overall larger, since it examined additional problems. Additional sources were consulted, but no relevant matches were found. For example, in 2020, the OECD compiled an overview of consumer detriment investigations undertaken between 2006-2018 across different jurisdictions, however, there were no relevant matches that could serve as a point of comparison for this Fitness Check. OECD (2020). 'Measuring consumer detriment and the impact of consumer policy: Feasibility study', OECD Digital Economy Papers, No. 293, OECD Publishing, Paris, April 2020.

[61] 'E-commerce sales of enterprises by NACE Rev.2 activity', Eurostat, April 2024. Percentage of Enterprises' turnover coming from web sales - B2C in NACE Rev.2 G47: Retail trade, except of motor vehicles and motorcycles in 2017 was 7.5%. Statista Market Insights estimates the share of online B2C retail of physical goods in 2017 at 8.4% of the total market.

approximately 8%. Using this percentage share, the online post-redress financial detriment from the Commission' 2017 detriment study was approximately EUR 2.7 billion, which is **very close to the estimations above.**

Furthermore, it is observed that the **increase in detriment resulting from online purchases over the evaluation period is consistent with the growth of the e-commerce market in the EU27 and average consumer spending online**. The B2C e-commerce market revenues grew by 85% between 2017 and 2023 from EUR 187.7 billion to EUR 347.3 billion. When divided by the number of consumers in the EU27 buying online, which is estimated by multiplying the total number of consumers in the EU27 (440 million) by the percentage of all individuals having bought online in the last 12 months, it is shown that the **average consumer spending online for those consumers that use the internet for purchases has increased by 43% from EUR 791 to EUR 1134.**

Table 5 - Evolution of the e-commerce market and average consumer spending online in the EU27 (2017-2023)

	2017	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
EU27 commerce revenue in billion EUR [62]	187.70	199.10	235.10	311.60	360.60	359.80	347.30
Internet purchases by individuals - Last online purchase: in the last 12 months - Percentage of all individuals[63]	53.90%	56.14%	59.79%	64.74%	67.11%	67.95%	69.60%
Average consumer spending per individuals having purchased online in the last 12 months in EUR	791	806	894	1 094	1 221	1 203	1 134

Source: DG JUST, estimations based on Eurostat and Statista Market Insights data

Other harms

The problematic practices identified in the Fitness Check can lead to multifaceted consumer harms beyond financial detriment that directly or indirectly impact the consumers' economic interests and the collective interests of consumers. The evidence base regarding the scale and severity of the risks that consumers face has been increasing over the evaluation period; however, scientific research is still evolving on certain emerging issues, especially given their relative novelty (e.g. addictive design, AI chatbots) or limited spread in mainstream consumer markets (e.g. virtual worlds).

However, it is important to note that EU consumer law, in particular the UCPD, **does not require there to be proof of actual harm occurring to consumers**. There needs to be an assessment of the likelihood of the impact that a commercial practice may have, in abstract, on the transactional decisions of consumers. Put differently, it is not necessary to prove a causal connection between a commercial practice and actual harm to individual consumers or an actual impairment of consumer autonomy in order to establish that a practice is unfair. Evidence of potential impairments and emerging risks over the evaluation period are therefore equally relevant to consider.

[62] 'eCommerce - EU-27', Statista Market Insights, May 2024.
[63] Internet purchases by individuals (until 2019)' and 'Internet purchases by individuals (2020 onwards)' Eurostat, March 2024.

The representative consumer survey for this Fitness Check collected data on whether consumers suffered any **mental harm** as a result of the problems they reported. **49% of the respondents reported experiencing a moderate level of distress, while a further 29% indicated quite a lot of distress**. Of those who indicated they experienced an 'extreme' amount or 'quite a lot' of distress, this was **higher among the older age groups**, while 36% of those aged 18-25 and 33% of those aged 26-35 indicated a high level of distress, this rose to 43% for those aged 46-55, 51% of those aged 56-65 and 49% for those aged 65+. This response was also particularly prevalent among those who have indicated they do not trust online businesses (55%), which highlights the **connection between non-compliance with consumer law and a reduction of consumer trust in traders**.

Figure 4 - Distress suffered by consumers due to problems experienced online in the context of commercial transactions[64]

Source: Consumer survey to support the Fitness Check

Dark patterns, manipulative personalisation and other unfair commercial practices that aim to influence consumers to take transactional decisions that may go against their best interests can lead to financial detriment but also to a **loss of autonomy and privacy, cognitive burdens, mental harm, and pose concerns for collective welfare due to detrimental effects on competition, price transparency and trust in the market**. In the representative consumer survey, respondents reported feeling confused (40%) and pressured (35%) by the exposure to dark patterns. The Commission's 2022 study on dark patterns and manipulative personalisation included behavioural experiments with a sample of 7430 consumers in six Member States (BG, DE, IT, PL, ES, SE) which showed that such practices not only impacted the consumers' decision-making (leading to financial detriment), but also **increased their levels of frustration, feelings of being manipulated, reducing their understanding of information, increasing distrust towards the website** etc. In addition, the study included a physical lab experiment with a sample size of 120 consumers in three Member States (IT, DE, ES) testing consumers' **neurophysiological and psychological reactions to dark patterns**. In the case of dark patterns that consist of forced action combined with personalisation (e.g. difficulties to close or skip a pop-up which contains personalised ads), the consumers' ability to take a decision was significantly hampered and their heart rate increased, which is associated with **increased anxiety and alertness**. While the Commission's exploratory research contributed to the evidence base on the impacts of such practices, there is a need for additional research in order to better understand the magnitude of the neurophysiological and psychological effects of different types of dark patterns. In its 2022 report, the OECD noted that while dark patterns often deceive, coerce or manipulate consumers and are likely to cause detriment in various ways, it may be *'difficult or impossible to measure such detriment in many instances'*.[65] Overall, even if the impact of a single unfair practice is not severe, the **constant exposure to misleading practices and micro-manipulations can lead to the gradual erosion of consumer trust**. A high level of consumer protection is not achieved if, as the Commission's study showed,

[64] 'To what extent have you felt emotionally distressed (e.g. angered, frustrated, or worried) as a result of the problem?' (n=2657)

[65] 'Dark commercial patterns: OECD Digital Economy Papers', No. 336, OECD Publishing, Paris, October 2022. Annex E of the OECD report provides an overview of selected evidence of financial loss, psychological detriment and impacts on consumer trust resulting from dark patterns.

consumers have come to accept the exposure to such unfair practices as part of their 'normal digital experience'.

Commercial practices such as addictive design (e.g. infinite scroll, loot boxes) and personalised recommender systems based on algorithmic profiling, which aim to keep consumers using the digital service for the purposes of increased data collection, sales and exposure to advertising, can lead to **time loss[66], attention-capture, 'rabbit hole' effects, various mental harms, such as anxiety and depression,[67] obsessive-compulsive symptoms, such as compulsive buying among young adults[68], or physical harm, such as problems resulting from a lack of sleep and sedentary behaviour which include a potential increased risk of early neurodegeneration[69]**. Although scientific research enabling to make a direct connection between specific features and these harms is still evolving, significant risks have been identified, in particular concerning the impacts of such practices on minors. A first exploration of such consumer harms in the context of EU consumer protection law has been carried out in the Italian authority's 2024 action against TikTok on the basis of the UCPD[70] and in the context of the 2024 proceedings related to risk assessments required from VLOPs such as TikTok and Meta under the DSA.[71] Digital addiction is currently not listed among substance-related disorders (e.g. smoking, alcohol), behavioural disorders (e.g. pathological gambling) or as a diagnosis in standard classifications.[72] Only gaming addiction has been formally recognised as a disorder.[73]

In its 2023 Communication on a comprehensive approach to mental health,[74] the Commission reported that the **annual value of lost mental health in children and young people is estimated at EUR 50 billion in the EU**.[75] The Communication underlined that the EU is

[66] Neyman C., 'A Survey of Addictive Software Design'. 1, 1, Article 1, June 2017.
[67] Twenge, J.M., Cooper, A.B., Joiner, T.E., Duffy, M.E., & Binau, S., 'Age, Period, and Cohort Trends in Mood Disorder Indicators and Suicide-Related Outcomes in a Nationally Representative Dataset, 2005–2017'. Journal of Abnormal Psychology, 128, 185–199, 2019. Learning to deal with Problematic Usage of the Internet, Revised Edition / COST Action 2023, See Internet Social-Media/Forum Addiction and others, p.18-19.
[68] Sohn, S., Rees, P., Wildridge, B., Kalk, N. J., & Carter, B., 'Prevalence of problematic smartphone usage and associated mental health outcomes amongst children and young people: a systematic review, meta-analysis and GRADE of the evidence'. BMC Psychiatry, 19, Article number 356.
Peterka-Bonetta, J., Sindermann, C., Elhai J.D., Montag, C., 'Personality associations with smartphone and internet use disorder: a comparison study including links to impulsivity and social anxiety', Front Public Health, Volume 7, Article 127, 2019.
Samra, A., Warburton, W. A., & Collins, A. M., 'Social comparisons: A potential mechanism linking problematic social media use with depression', Journal of Behavioral Addictions, Macquarie University, Australia, Volume 11, Issue 2, 2022.
Stéphanie Laconi et al, 'Cross-cultural study of Problematic Internet Use in nine European countries', Computers in Human Behavior, Volume 84, July 2018, pp.430-440.
Lopez-Fernandez, O. & Kuss, D., 'Harmful Internet Use Part I: Internet addiction and problematic use', European Parliament Research Service - EPRS, Scientific Foresight Unit - STOA, January 2019, p. 51.
Cesarina Mason, M., Zamparo, G., Marini, A., A., Nisreen, 'Glued to your phone? Generation Z's smartphone addiction and online compulsive buying', Computers in Human Behaviour, Volume 136, November 2022
[69] Neophytou, E., Manwell, L.A., Eikelboom, R., 'Effects of excessive screen time on neurodevelopment, learning, memory, mental health, and neurodegeneration: a scoping review Int J Ment Health Addiction, 19, 2019, pp. 724-744.
[70] 'TikTok sanctioned for an unfair commercial practice', Autorita Garante della Concorrenza e del Mercato, March 2024.
[71] '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', European Commission, April 2022.
'Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram', European Commission, May 2024.
[72] Not listed in the Diagnostic and Statistical Manual of Mental Disorders (DSM-V) or the International Statistical Classification of Diseases and Related Health Problems (ICD-10/ICD-11).
[73]The 'Gaming Disorder' (GD) features in the WHO' eleventh International Classification of Diseases
[74] Communication from the Commission to the European Parliament, the Council, the European Economics and Social Committee and the Committee of the Regions on a comprehensive approach to mental health of 07.06.2023, COM(2023) 298 final.
[75] 'The State of the World's Children 2021: On My Mind – Promoting, protecting and caring for children's mental health', United Nations Children's Fund (UNICEF), October 2021.

witnessing a worsening of the mental health of its younger generations and that suicide is the second leading cause of death among young people (15-19 years of age)[76] after road accidents.[77] The Communication stressed that **a comprehensive approach to mental health must recognise the role of economic and commercial factors (e.g. pressure from aggressive marketing) as determinants of mental health**. While it was recognised that digital tools can also have a positive impact on mental health, there is a need for more effective safeguards against harmful content, aggressive marketing, excessive screentime and an imbalanced use of gaming.

Commercial marketing practices that are based on the creation of **parasocial relationships between consumers and social media influencers** can exacerbate the commercial pressure that consumers feel, even if there were to be full disclosure about the presence of commercial communications. In this context, endorsements of potentially problematic products and services, such as health supplements with dubious claims about preventing illnesses, can lead to multifaceted harm, especially if they reach vulnerable consumers such as minors or exploit vulnerabilities such as health issues. Also, influencer marketing may pose risks to mental health by fostering unrealistic expectations, including about consumer consumption, thereby contributing to stress and anxiety. Exposure to idealised lifestyles, curated content and feedback-seeking behaviours can lead to feelings of inadequacy, anxiety, addiction to social media and depressive symptoms.[78]

Consumers may also be more perceptive to undue influence (e.g. hidden advertising, pushed to conclude microtransactions) when they are **immersed in gameplay or virtual world environments**. Video games and gaming platforms have increasingly become a type of online marketplace for minors, which operates with alternative 'currencies' that could distort the comprehension of the fact that consumers are taking transactional decisions in a commercial environment and the real price of each individual purchase.

The use of **emotion-recognition AI or anthropomorphic AI systems** that emulate human communication and emotions can unduly distort consumers' decision-making, even if consumers were to be fully informed that they are subject to an emotion-recognition system or that they are interacting with AI. Furthermore, generative AI can learn consumer behaviours and produce content that mirrors their interests and emotional states, which could enable a more effective targeting of vulnerabilities and make content particularly addictive.[79]

More broadly, the **use of big data and AI can be used to appreciably limit consumer autonomy**, thereby putting into question the image of a reasonably rational and observant consumer that underpins EU consumer law. Undue influence can be exercised in myriad ways, e.g. through interface design and functionality decisions in the **development of virtual assistants** such as the determination of the pitch, rate and volume of the voice, putting more emphasis on some options than others, emulating personality treats and perpetuating gender stereotypes.[80] The ability to make adequately informed choices in light of their reasoned preferences is challenged by the possibility to influence consumers' choices, possibly without

[76] 'The State of the World's Children 2021: On My Mind – Promoting, protecting and caring for children's mental health', United Nations Children's Fund (UNICEF), October 2021.
[77] Keles, B., McCrae, N., and Grealish, A., 'A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents', International Journal of Adolescence and Youth, Volume 25, No. 79-93, 2020.
[78] Mundel, J., Yang, J. and Wan, A., 'Influencer Marketing and Consumer Well-Being: From Source Characteristics to Social Media Anxiety and Addiction', The Emerald Handbook of Computer-Mediated Communication and Social Media, June 2022.
[79] Greenfield, D. and Bhavnani, S., 'Social media: generative AI could harm mental health', Nature Journal, May 2023.
[80] Naidu, S., and Mohandas, S., 'Deceptive Design in Voice Interfaces: Impact on Inclusivity, Accessibility, and Privacy', The Unpacking Deceptive Design Research Series, The Pranava Institute, 2023.

them being aware of such influence.[81] Consumer may be hyper-nudged into choices that they can regret, especially if their vulnerabilities are exploited.[82] As a result, consumers may be induced to **purchase goods they do not need, to overspend, to engage in risky financial transactions or to indulge in their weaknesses**, which can lead to harm beyond financial detriment.[83]

As a cross-cutting issue, all of the products and services offered in the digital environment are accompanied by contract terms that the majority of consumers never read. The **lack of transparency and fairness in standard contract terms** can also result in consumer detriment going beyond financial harm. In the representative consumer survey, consumers reported **lost time** because it was not clear where to find the T&Cs on the website/app (35%), having their **privacy harmed** because T&Cs led them to share more personal data than intended (29%), **losing access to the service or to their account** because they did not know the relevant T&Cs (23%) or having **difficulties with exercising their rights** because it was hard to understand which T&Cs apply to their contract (32%).

Finally, the magnitude of the various problematic practices and the potential harm that they could create is **exacerbated by their speed, scale and potency to influence a large number of consumers in a short amount of time in the digital environment**. Although many of these practices, especially persuasive marketing techniques, are also prevalent in the offline world, the exponential development of technology over the evaluation period has amplified and deepened the types of risks within the scope of the three Directives and increased the possibility of potential harm occurring both to the individual and collective interests of consumers.

Implementation and application

From a legal perspective, all three Directives continued to be **properly implemented at national level** during the evaluation period, without any major issues specifically concerning the application of the rules in the digital environment. However, case law and enforcement actions applying the rules in the digital environment have remained limited, especially concerning novel or data-driven practices.

At European level, the Consumer Protection Cooperation (CPC) Regulation enables national authorities to coordinate their views and **tackle infringements of EU consumer law with a cross-border dimension**. There have been several coordinated actions concerning digital practices by online platforms, marketplaces, messaging services, dating apps and travel booking intermediaries, which resulted in commitments from traders to improve compliance. For example, when e-commerce problems were temporarily exacerbated during the COVID-19 pandemic (especially as regards increased reports of misleading online advertising, scams and fraud), the CPC network requested online platforms to better identify, remove and prevent the reappearance of millions of illegal practices.[84] The remaining obstacles to the effective public enforcement of the three Directives, including specifically in the digital context, are specifically tackled in the application report on the CPC Regulation published on 25 July 2024.[85] The challenges with consumer ADR are under examination in the revision of the ADR Directive,

[81] Calo, R., 'Digital market manipulation. George Washington Law Review', 82:995, 2013.
[82] Mik, E., 'The erosion of autonomy in online consumer transactions. Law, Innovation and Technology' 8, 2016, pp. 1–38.
[83] 'New Aspects and challenges in consumer protection, Digital services and artificial intelligence', European Parliament, PE 648.790 April 2020.
[84] 'Coronavirus: following Commission's call, platforms remove millions of misleading ads', European Commission, Press release May 2020.
[85] Report on the application of Regulation (EU) 2017/2394 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws, COM(2024) 311 final.

following adoption of the Commission's proposal of 17 October 2023.[86] In area of private enforcement, the application of the Representative Actions Directive as from 25 June 2023 did not yet result in collective injunction or redress cases in digital markets. The impact of enforcement on the effectiveness of the three Directives is further analysed in section 4.1.1.3.

The evaluation period included the entry into application of the **Modernisation Directive** on 28 May 2022, which introduced new amendments to all three Directives in response to the problems identified in the previous 2017 Fitness Check and CRD evaluation. The amendments included targeted new measures concerning the digital environment, such as ensuring the transparency of product ranking in search results, online consumer reviews, personalised pricing and selling arrangements on online marketplaces. The Modernisation Directive also introduced stronger remedies and penalties for consumer law breaches. In parallel to this Fitness Check, the Commission prepared the implementation report on the Modernisation Directive, which enabled synergies for both analyses.[87] The report concluded, among others, that the evolution of consumer online markets and new technologies pose challenges and require strong monitoring.

Additional relevant changes included the application of the Digital Content Directive, Sale of Goods Directive, General Data Protection Regulation and revised Audiovisual Media Services Directive. More recently, the broader legislative framework for digital markets was strengthened by the application of the Digital Services Act and Digital Markets Act, which, among others, lay down rules concerning the commercial practices of online intermediaries and digital gatekeepers. More changes are forthcoming with the entry into application of the AI Act, Data Act, European Accessibility Act, revised Product Liability Directive, and proposal for an AI Liability Directive, among others. Additional analysis of the interplay with EU consumer law is provided in section 4.1.2.2 on external coherence and in Annexes VI and VII.

Beyond legislation, work has evolved on voluntary codes of conduct in the area of EU consumer law, such as the **Consumer Protection Pledge** of 30 November 2023, which includes specific digital rights commitments from large online marketplaces as regards: facilitating the exercising of the consumer's right of withdrawal and cancellation, enabling access to human interaction in customer service, measures promoting transparency of influencer marketing and reliability of consumer reviews, and informing and training sellers about EU consumer law. However, this initiative only concerns a limited number of specific type of actors (online marketplaces) that signed up to it. Furthermore, in 2023-2024 the Commission facilitated stakeholder dialogue under a **Cookie Pledge** to agree voluntary pledging principles regarding cookies and other similar technologies capable of tracking users' online navigation. The overall objective was to counter 'cookie fatigue' and empower consumers to make more effective choices regarding tracking-based advertising models. However, while this initiative did not result in signatures from the market players in 2024, as it proved impossible to achieve self-regulatory commitments on this complex consumer protection matter, the principles discussed within the project constitute a set of well-balanced solutions that could guide stakeholders towards more transparent and responsible practices.

Against the general state of play described above, the following sections will provide an analytical account of the success or failure of the three Directives in achieving their objectives in the digital environment and examine more closely the problems identified.

[86] 'New measures to simplify the resolution of disputes out of court and boost consumer rights', European Commission, Press Release October 2023.
[87] Report on the implementation of the Directive on the better enforcement and modernisation of Union consumer protection rules, COM(2024) 258 final.

4. Evaluation findings

4.1. To what extent was the intervention successful and why?

The key findings are summarised in the table below per evaluation criterion, together for all three Directives:

Table 6 - Summary overview of the key evaluation findings per criterion

Evaluation criterion	**Summary assessment[88]**	**Key findings**
Effectiveness	Limited	- Consumer complaints and detriment remain high[89]; problems are amplified by the increased scale, speed and potency of digital solutions for targeting consumers - Legal uncertainty regarding the application of the laws and gaps of protection in certain areas - Risk of regulatory fragmentation due to diverging interpretations and national laws in certain areas - Insufficient public and private enforcement
Coherence	Positive with limitations	- Internal coherence: consistent and mutually reinforcing - External coherence: generally complementary to other EU legislation but it is important to ensure coherent interpretation of key concepts when applying the different regulatory frameworks
Efficiency	Positive with limitations	- Costs and benefits are balanced at societal level (to the extent that they are quantifiable and attributable) - Compliance costs for businesses are generally not considered to be high[90] - Significant benefits for consumers, traders and authorities (e.g. consumer protection and trust in digital markets, more regulatory certainty through harmonisation and enabling cross-border enforcement cooperation) - Specific areas with potential for simplification (e.g. information obligations, right of withdrawal)
EU added value	Positive	- EU legal framework achieves moderately or significantly better outcomes than could have been achieved by Member States
Relevance	Positive with limitations	- Objectives remain highly relevant - Benefits of a technology-neutral safety-net framework - Different technological and market developments will have an impact on fitness for purpose and are expected to

[88] Assessment categories: positive/positive with limitations/limited/negative.
[89] Financial post-redress consumer detriment resulting from problems in the digital environment is estimated at approximately EUR 7.9 billion per year.
[90] Adjustment and administrative costs associated with compliance with the Directives amounts to approximately EUR 511-737.3 million per year. Only 10-18% of traders report high costs relating to the different compliance activities, whereas the majority face low costs or no costs at all.

		do so at a faster pace in the future (e.g. growing use of AI, automation, personalisation) - Application of other EU legislation will impact relevance

Source: DG JUST, based on the overall conclusions of this Fitness Check

4.1.1. Effectiveness

4.1.1.1.*Achievement of the objectives*

The Fitness Check confirms that the three Directives under evaluation in the horizontal EU consumer protection framework have provided the necessary minimum of regulatory certainty and consumer trust to support the development of a diverse market of consumer-facing digital products and services in the EU. The Directives have contributed to these outcomes through the technology- and channel-neutral legislative approach as well as the combination of principle-based rules and concrete prohibitions/obligations, with a mix of minimum and full harmonisation provisions. Overall, the Directives can be considered to have been **partially effective in the digital environment**; however, their functioning is undermined by a lack of compliance by traders (which leads to consumer detriment), ineffective enforcement, legal uncertainty, regulatory fragmentation, compounded by the increased complexity of the rapidly changing regulatory landscape with the arrival of new legislation.

Concerning the **objective of providing a high level of consumer protection**, the persistence of a large volume of consumer complaints and consequent consumer detriment over the evaluation period shows that the Directives have only partially achieved this objective. Concerns remain even if the number of complaints and detriment is lower than what could have been expected, taking into account the massive growth of digital markets. The scale and development of the problematic practices over the evaluation period was analysed in section 3 and in more detail, per practice, in Annex VI. Consumer awareness of their rights remains insufficient and those who encountered problems continue to be deterred from taking action to resolve the problems and obtain redress.

In the digital environment, EU consumer law can apply not only when consumers engage in purchasing decisions, but also in their broader capacity as users or recipients of commercial practices, i.e. when they get access to 'free' digital content or services (under the condition of agreeing to use their personal data), when they are exposed to advertising or when they decide to spend more time or attention using a specific service. So far, the impact of EU consumer law has been most evident in the immediate context of purchasing decisions and advertising, but its **potential has remained underexplored in situations where consumers provide their data and spend their time**.

Traders' non-compliance with the three Directives in the digital context is difficult to measure directly, given the absence of reporting requirements in the Directives, longitudinal datasets from public or private sources, and the very wide range of issues covered by the Directives' material scope. However, representative datasets of consumer complaints and detriment are a key indicator for measuring compliance in practice. As outlined in section 3, there has been an increase of consumer detriment over the evaluation period, even when accounting for inflation and e-commerce growth. Additionally, the compliance assessments in sweeps (i.e. EU-level CPC sweeps by authorities, targeted investigations conducted for this Fitness Check and data from secondary research) show that there is still considerable scope for improving traders' compliance with the existing rules in the digital environment. In terms of stakeholder perceptions on achieving the specific objectives of the three Directives, the existing rules can

be considered to have been at least **partially effective in tackling a variety of problematic practices, such as transparency in advertising and pre-contractual information**. For example, respondents to the targeted stakeholder survey considered that the compliance level is high regarding the 14-day right of withdrawal (71%) and pre-contractual information (57%), whereas the highest figures for non-compliance concerned the requirements regarding price reductions (22%) and unfair standard contract terms (21%). While 44% of respondents considered that there is a possibility for traders to bypass certain obligations in EU consumer law using contractual, technical or behavioural measures, 29% considered this to be true only to a small extent and 28% not at all.

The areas where consumer law was perceived as having been **less effective in addressing problems mainly concerned emerging technologies and practices for which there are no specific provisions in the Directives**. As exemplified by interviews, position papers submitted in the public consultation and the percentages of responses to the targeted stakeholder survey, the highest levels of ineffectiveness were flagged regarding the unfair use of AI systems for commercial purposes (64% ineffective overall), problems concerning the addictive use of digital products and services (62% ineffective), the use of consumers' data that exploits specific vulnerabilities for commercial purposes (60% ineffective), the use of loot boxes and addiction-inducing features (59% ineffective) and problems with the automatic conversion of free trials into paid subscription contracts (58% ineffective). The correlation between the areas that are deemed as being least effectively tackled and the absence of specific rules in the three Directives addressing them points to the limits of the principle-based approach.

In terms of the situation in individual Member States, the consultations and data collection **did not indicate any significant differences regarding the relative scale of the explored problematic practices between Member States**. The lack of significant differences can be explained by the fact that the common marketing and sales practices in the digital environment are relatively heterogeneous, and the majority of the most popular websites and apps used by EU consumers are operated by the same providers (certain aspects will differ, such as the regional T&Cs, language and delivery options).[91] Based on the representative consumer survey results, which covered 10 Member States, there were slight divergences reported, but overall, the average consumer experience across the EU appears to be rather heterogenous in the digital environment. For example, in most Member States, 31-47% of consumers felt pressured to buy something due to dark patterns, while the figure was slightly smaller among French consumers (22%). Consumers reported seeing potentially misleading scarcity claims (e.g. low stock, limited availability) to a high extent across the different Member States (54-69%), with especially high figures in Portugal (70%) and Romania (74%). Difficult cancellations were reported most by consumers from Sweden (52%), whereas 33-43% of consumers from other Member States reported experiencing the same. Hidden advertising by social media influencers was reported by 40-51% of consumers in most Member States, whereas French consumers experienced such practices slightly less (32%), which could be at least partially attributed to the active enforcement at national level.

There were also small differences in how important consumers consider their rights and how often they exercise them in different Member States specifically in the digital environment. In the representative consumer survey, when questioned about how important they feel consumer rights are for decisions related to the purchase or use of a product or service online, 48% of all consumers felt they are 'very important' whilst a further 43% indicated them to be' important'. On a country level this was most important for consumers from Portugal (91%), whilst it was

[91] For example, in 2022, among the top 30 most visited websites relevant for consumer law (based on SE traffic, i.e. number of visitors coming to a site from organic search results), there were only 8 national sites, whereas 22 were servicing the EU as a whole.

least important in Spain and Estonia (77% and 76% respectively). However, despite the majority of consumers indicating that they are aware of the importance of their consumer rights, approximately 60% of all consumers surveyed indicated they had not been previously able to use consumer law to ensure respect for their rights in the digital context. On a country level, individual consumers were least active in France (18%) and Hungary (23%), whereas consumers were most active in Romania (36%) and Estonia (31%). Those in the older age cohorts were most likely to indicate inactiveness; 74% of respondents aged 65+ and 67% of those aged 56-65, compared to 46% of those aged 18-25 and 48% of those aged 26-35. On average, across the three lowest-income quartiles 65% of respondents indicated they had not been able to use the legislation compared to an average of 55%.

In addition to the differences in consumer perceptions, there were differences in the perception of business costs between traders in different Member States (see section 4.1.3.1 on efficiency). Moreover, there are differences in administrative capacities and resources for consumer authorities, which affects public enforcement (see section 4.1.1.4), although it was not possible to quantify and compare such differences.

The **objective of ensuring the better functioning of the internal market through the harmonisation of rules** has also been only partially achieved. In areas where the Directives prescribe specific rules, there are, to varying degrees, problems with uniform interpretation and application, including sub-optimal compliance by market participants. In areas in which the Directives are less prescriptive or silent, there are instances of legal gaps or legal uncertainties, and, in the absence of EU action, an emergence of national laws and other measures that could create obstacles for cross-border trade.

In order to better address some of the problematic practices identified in the Fitness Check, some Member States have started to unilaterally regulate the issues and national authorities have developed different interpretative guidelines and recommendations. While the adoption of legislative or non-legislative national measures aimed at increasing consumer protection in the digital environment (e.g. concerning digital contracts, influencer marketing, loot boxes) can be viewed as a measure that reduces consumer harm, it can also lead to **regulatory fragmentation that undermines the Digital Single Market**, as traders face increased costs related to the familiarisation with the rules and their implementation. Regulatory fragmentation can disproportionately affect smaller traders. Legal barriers can prevent smaller companies from operating or scaling up, thereby giving a competitive advantage to larger companies that are better equipped to face these costs and operate cross-border. An increase in legal liability and uncertainty can also lead to risk-avoidance behaviour that prevents traders from innovating. Regulatory fragmentation also creates confusion for consumers and makes it more difficult for them to understand their rights when they are faced with different commercial practices depending on the Member State where they shop.

The problems with legal uncertainty and ineffective enforcement are explained in separate sub-sections 4.1.1.3 and 4.1.1.4. In brief, the application of the three Directives to novel digital practices is subject to considerable legal uncertainty and the enforcement of the laws cannot be considered sufficiently effective in the digital environment. The underlying enforcement problems are multifaceted and include a lack of financial resources, however, the 'enforceability' of the substantive legal framework plays a key role. There is a lack of clarity about how the principle-based general provisions should be applied in concrete cases, in addition to excessive difficulties with meeting the burden of proof in technologically complex cases (e.g. proving the occurrence of an unfair practice in case of personalisation targeted towards specific consumers) and a lack of incentives for traders to take technical and

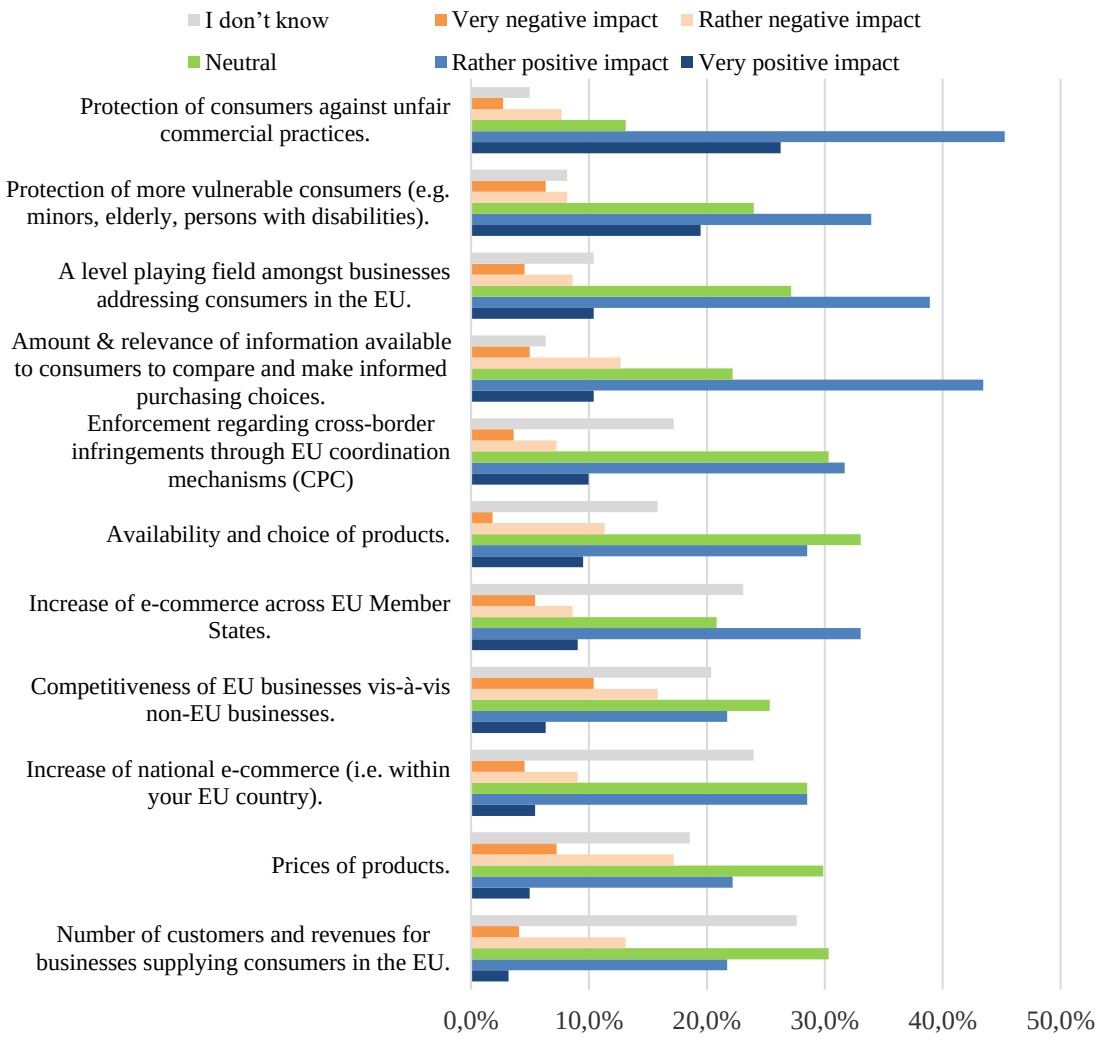
organisational measures to incorporate consumer protection considerations at all stages of the product or service development.

Several of the problematic practices identified in the Fitness Check represent a case of market failure involving asymmetric information between consumer and traders, which allow traders to impose unfavourable conditions. Consumers are at a disadvantage when traders engage in misleading practices (e.g. hidden influencer marketing), impose unfair contract terms or deploy techniques to exploit their biases (e.g. dark patterns, personalisation based on vulnerabilities). As a result, consumers could buy unsuitable products/services, pay too much, not have their expectations met and potentially not participate in some segments of the market (e.g. not seeing the full selection of available products/services due to personalisation). Competition can be negatively impacted when consumers are unfairly steered towards a limited amount of traders or products/services, as well as when non-compliant traders obtain a competitive advantage over compliant traders by bypassing the rules or by making use of legal uncertainty and loopholes. The Fitness Check has shown that there is **additional scope for removing or limiting the impacts of such market failures through EU consumer law in the digital environment** in order to see more positive economic and societal effects for both consumers and law-abiding traders.

The Fitness Check has shown that the necessity for the safety-net consumer protection framework, as currently established in the three Directives, was not put into question by any stakeholder. In fact, there was a consensus among the stakeholders during interviews and in responses to the consultations that a strong legal framework is required to protect consumer interests in the digital environment. EU consumer law provides clear added value next to other sector-specific and technology-specific digital legislation. The legal requirements in the Directives reflect the usual behaviour that can be expected from diligent traders acting in good faith. Many stakeholders also considered that, in general, **the existing legal framework can provide sufficient protection in the digital environment, if it is properly enforced in practice**. However, the synthesis analysis of stakeholder positions reveals a complex and dynamic landscape - while there is general agreement that strong consumer protection laws are necessary, there are divergent views on both the state of play of the current legislative framework and the need for further legislative changes, which are further explored in the sub-sections on external coherence (4.1.2.2) and relevance (4.3).

As illustrated by the graph below, in the public consultation, the three Directives were perceived to have had a positive impact on achieving a variety of general and specific objectives in the digital area. Concretely, positive impacts were identified as regards protecting consumers against unfair commercial practices (71%), protecting vulnerable consumers, e.g. minors, elderly, persons with disabilities (53%), increasing the amount and relevance of information available to consumers to compare and make informed purchasing choices (54%), contributing to a level playing field among businesses addressing the needs of consumers (49%), increasing cross-border e-commerce (42%) and enabling the enforcement of cross-border infringements through the CPC network (42%). In contrast, the perceptions were more varied concerning the impacts of the Directives on increasing national e-commerce and competitiveness of EU vs. non-EU businesses, with a significant proportion of respondents being neutral (25-29%). Likewise, the impact on the prices of products and the number of customers and revenues for businesses supplying consumers in the EU were varied, with the largest part being neutral (30%). These perceptions indicate that the Directives have had a **more immediate impact on consumer protection in terms of enhancing the available information and protection against certain unfair practices**, whereas the **impact is less discernable on market factors such as the level of prices, competitiveness or traders' turnover**.

Figure 5 - Stakeholder perceptions of the impact of the Directives in the digital environment[92]



Source: Public consultation to support the Fitness Check

4.1.1.2.*Competitiveness, innovation and impact on SMEs*

The dual objectives of EU consumer law – ensuring a high level of consumer protection and a better functioning of the internal market through harmonised rules – have a direct impact on competitiveness in digital markets. A level playing field in the Digital Single Market can enable traders to grow and achieve the necessary scale to compete at EU level, while also guaranteeing that new technologies and digital services work for consumers. Ensuring a high level of consumer protection can have positive effects on competitiveness and innovation, as stated the 2024 **Letta report**: *"Strengthening these measures not only ensures fair access to goods and services across member states but also fosters a competitive environment that benefits both consumers and businesses. As the EU continues to adapt to changing consumer preferences and economic challenges, robust protections will secure the resilience and integrity of the Single Market, ensuring it remains a cornerstone of European prosperity and innovation."*[93]

[92] "How positive / negative is the impact of the existing EU consumer law framework on the following aspects in the digital environment?" (n=221)

[93] Letta., E., 'Much More than a Market: Speed, Security, Solidarity – Empowering the Single Market to Deliver a sustainable future and prosperity for all EU Citizens', April 2024.

However, while effective consumer policy is a necessary component of ensuring competitive digital markets, it could potentially have negative or unintended impacts on competitiveness and innovation in certain cases, e.g. if it creates regulatory requirements that are costly or difficult to comply with or if it restricts price competition or advertising.[94]

Concerning the overall magnitude of the burdens imposed by the three Directives under evaluation in this Fitness Check in the digital context - as shown in more detail in section 4.1.3.1 on efficiency - **the majority of traders, including SMEs, consider the regulatory burden to be modest**.[95] **In general, the Directives are not costly or difficult to comply with, nor are they perceived to unduly restrict price competition or advertising.** As these Directives have been in force for over 10-30 years, the initial one-off expenditures were largely experienced in the past, outside of the evaluation period. It has not been possible to identify any negative impact of the consumer protection obligations in the Directives on the growth of e-commerce and digital markets until now; to the contrary, the introduction of measures such as the CRD's 14-day right of withdrawal from online purchases has directly increased consumer confidence in purchasing online and the prohibition of misleading advertising has prevented unfair competition between traders. Recurring compliance costs for law-abiding traders are modest and the Directives do not contain any reporting obligations for traders towards the Member States or the Commission. Traders mainly experience costs when they conduct regular compliance checks, or if they intentionally or negligently breach the law and consequently have to take measures to bring their practices into compliance, or in case they are new players in B2C digital markets and have to familiarise themselves with the existing rules, or in case there are new amendments to the rules that they have to familiarise themselves with (e.g. by the MD or 2023 DMFSD revision).

In addition, the compliance burden has been alleviated thanks to various measures that the **Commission and national authorities take to support traders in their compliance efforts**, such as providing guidelines, engaging in preventative enforcement dialogues and funding projects to educate SMEs on consumer law. The SME training project "Consumer Law Ready" has educated in the last six years more than 2100 trainers in the EU on consumer law, who have subsequently trained thousands of SMEs at national level. The project is highly appreciated by trainers and SMEs for the hands-on approach and the quality of the material, which covers the obligations in the three Directives and additional laws. In 2024, the project is expanding to Ukraine and the Western Balkans. Given the diversity of traders that are subject to EU consumer law, the necessary approach may differ per type of trader. For example, for social media influencers, in 2024 the Commission created a dedicated Influencer Legal Hub with video training and resources that help them understand their legal requirements. Support for traders during their compliance activities is essential for ensuring consumer protection in practice.

[94] '[Measuring consumer detriment and the impact of consumer policy: Feasibility study](), OECD Digital Economy Papers, No. 293, OECD Publishing, Paris, April 2020.

[95] As explained further in section 4.1.3.1, only a minority of traders report facing high costs of compliance. Regarding the costs associated with the familiarisation with the rules, around 14% of companies with 1-9 employees, 19% of companies with 10-49 employees, 23% of companies with 50-250 employees and 27% with more than 250 employees declared that they face high compliance costs. Regarding the costs associated with the checking of business' compliance with the legal requirements, around 9.5% companies with 1-9 employees, 20% of companies with 10-49 employees, 29% of companies with 50-250 employees and 23% with more than 250 employees declared that they face high compliance costs. Regarding the costs associated with the information obligations, around 7.5% of companies with 1-9 employees, 14% of companies with 10-49 employees, 21% of companies with 50-250 employees and 13% with more than 250 employees declared that they face high compliance costs. Regarding the costs associated with adjusting business practices, around 6.5% of companies with 1-9 employees, 15% of companies with 10-49 employees, 17% of companies with 50-250 employees and 12% with more than 250 employees declared that they face high compliance costs.

Consumer trust in traders plays a key role in ensuring competitiveness and innovation. Studies have shown that **empowered consumers can drive innovation,** as respecting consumers' rights and values is essential to gaining consumer trust. For example, the global Trust Barometer published by the Edelman Trust Institute in 2023 (in Europe examining FR, DE, UK) indicated that consumer trust drives business growth as consumers reward the brands they trust with purchase and loyalty. According to the study, consumers consider trust in the business or brand to be the third most important deciding factor when making a purchase.[96] Trust in companies and a general alignment with their values is particularly important to the younger generation of consumers. 59% of consumers surveyed are more likely to buy new products introduced by a brand if they trust it and 67% are more likely to show loyalty and return to purchase to brands they trust.[97] These conclusions are reinforced by the findings of Forrester's extensive research conducted on a global scale into consumers' trust (e.g. in Europe examining FR, DE, IT, ES, SE and the UK), as reported by Forbes. Forrester also found that **the higher the level of consumer trust in a company, the higher the potential for innovation as there is an increased likelihood of return to purchase, trial of unrelated products, and willingness to share personal data**.[98] In addition, PwC conducted its biannual global consumer insights survey in 2023 (in Europe examining FR, DE, IE, ES), which showed that consumer trust is equally crucial when it comes to sharing personal data with companies, which allows them to gain valuable insight that propels innovation and boosts competitiveness as they thrive to become more efficient and provide better value for consumers on the basis of the data received.[99] 49% of those surveyed by PwC do not share more personal data than what is necessary due to a lack of trust in its protection by traders. However, the more trust consumers have in a company, the more data they are willing to share, leading to business growth and increased competitiveness. These findings point to the importance of ensuring a high level of consumer protection in the three Directives as a driver of innovation.

The European Parliament's 2019 study provided an analysis of the available evidence on the economic benefits related to key EU consumer protection legislation, which are relevant for assessing the impacts on competitiveness.[100] The analysis showed that **stronger consumer laws provide a positive wider economic impact and the effects can be quantified in certain areas.** However, it was acknowledged that quantitative estimates of effects on a general macroeconomic level (such as a change in GDP, employment or measures of consumer welfare) are limited. In most cases, such effects can be inferred from economic theory and supplied evidence that a given regulation works on the microeconomic level. The relative scarcity of quantitative evidence results from reasons such as difficulty in disentangling effects of regulation, lack of data, effects being dispersed, difficulty in quantifying the impact of qualitative changes and the inherent imperceptibility of some effects, especially preventive ones. Nevertheless, some **targeted examples of observed and estimated effects** are provided below based on the available data. For example, the EP study showed that, concerning effects on GDP and employment, different EU consumer protection measures were envisaged to contribute to additional economic output. Available estimates refer to a GDP increase of up to 1.0% per year, usually around 0.1%.[101] Some additional employment can be expected, with certain regulations having a direct positive impact on jobs, estimated at a few thousand new

[96] 'The Collapse of the Purchase Funnel', Edelman Trust Institute, Edelman Trust Barometer Special Report, 2023 p. 9.
[97] Ibid., p. 20.
[98] 'Consumer Trust: A Key Driver For Business Growth In 2023', Forrester, Forbes, June 2023.
[99] 'Consumer seek frictionless experiences in a world of disruptions', PwC, Global Consumer Insights Pulse Survey, February 2023.
[100] 'Contributions to Growth: Consumer Protection – Delivering economic benefits for citizens and businesses', European Parliament, PE 638.396, May 2019.
Directly relevant in the case of the CRD and by analogy for the UCPD and UCTD.
[101] For example, the Impact Assessment for the DCD envisioned a GDP increase of 0.03% or about EUR 24billion in 10 years.

jobs.[102] The numbers that were provided in available studies may be considered an underestimation in some cases, as they often cover only jobs directly necessary for ensuring compliance and do not include additional employment due to an increase of general economic activity. Concerning effects on sales and trade, consumer protection measures targeted at online activities were expected to provide additional online purchases of the magnitude of several per cent each.[103] For the time period of 2014-2017, the 3% growth of online purchases was partly attributed to the CRD and it was estimated that EUR 27.5 thousand per trader can be saved due to reduced diversity among the laws of Member States. Concerning effects on prices and consumer consumption, price estimations pointed at a reduction of up to 1% and additional consumer surplus/benefits were provided up to EUR 3 billion a year across the different EU consumer protection measures.[104] The amendments by the Modernisation Directive to the three Directives were estimated to improve consumer welfare because the costs of infringements were shifted to infringers and costs of obtaining redress for consumers were lowered. Furthermore, there was estimated to be a positive impact on vulnerable consumers (in particular persons with disabilities, elderly people or people with a migrant background) and a more level playing field for law-abiding traders, leading to more competition, innovation and investment, although these effects were not quantified. As an additional source of evidence, a 2020 academic study, which utilised data *inter alia* from Eurobarometers and Eurostat, found there to be between 2006-2014 a significant relationship between the introduction of the UCPD and consumer trust and cross-border purchases in Member States with a low level of consumer protection prior to the introduction of the UCPD.[105] In general, the results implied that improved and standardised consumer protection within the EU has positive effects on trust that consumers have vis-à-vis traders and public authorities, and specifically on online purchases.

The public consultation for this Fitness Check explored stakeholder perceptions about the extent to which the application of the three Directives in the digital context has impacted competitiveness. Respondents considered there to be a positive impact of the Directives on contributing to a level playing field among businesses addressing the needs of consumers (49% positive impact) and increasing cross-border e-commerce (42% positive impact), which are **crucial for intra-EU competitiveness**. However, the **perceptions were more mixed concerning the impacts on increasing competitiveness of EU vs. non-EU traders, with a significant proportion of respondents being neutral** (25-29%).

EU consumer legislation applies to all business-to-consumer relationships in the internal market, **regardless of the origin or establishment of the trader**. This means that it applies both to traders established in the EU and to traders based outside the EU who target consumers in the EU, where it is apparent from the website and the non-EU trader's overall activity that it intends to engage with consumers in the Member States e.g. because of the international nature of the activity, use of a language and currency (for example the euro) of the Member States, a domain name registered in one of the Member States, geographical areas in the EU to which dispatch of a product or provision of a service is possible.[106] Challenges mainly arise when a

[102] For example, the DCD envisioned a net increase in employment level of around 60,000 jobs, given the positive effects on trade and consumption.

[103] For example, online cross-border sales were expected to grow up to 14% in case of DCD, while other estimations were more modest.

[104] For example, in the case of the DCD, an increase of up to 0.23% was estimated for the growth of private consumption

[105] Rösner, A., Haucap, J., & Heimeshoff, U., 'The Impact of Consumer Protection in the Digital Age: Evidence from the European Union', International Journal of Industrial Organization, 2020. The effects become stronger over time, peaking for trust outcomes in 2012. The results passed several robustness tests, including controlling for time invariant effects, changes on model specification and tests on treatment and control group.

[106] See by analogy the judgment of the CJEU of 12 July 2011, Case C-324/09 *L'Oréal v eBay*, paragraph 65 and judgment of the CJEU of 7 December 2010 in Joined Cases C-585/08 and C-144/09 *Peter Pammer* (C-585/08) *and Hotel Alpenhof* (C-144/09).

non-EU trader does not have any establishment or assets in the EU, which means that enforcement needs to take place abroad, beyond the jurisdiction of the national consumer authority. The **growth in the number of non-EU traders targeting EU consumers poses enforcement challenges that undermine the effectiveness of the Directives.** Coordinated enforcement in the CPC network has a more limited impact on non-EU traders due to, among other factors, a lack of cooperation agreements with third countries. Overall, it is important to highlight that the possible competitive disadvantage between EU vs. non-EU traders does not stem from the obligations in the three Directives, but rather from the difficulties in ensuring effective enforcement in practice. The 2024 application report on the CPC Regulation pointed to this challenge in the context of reflections on the future of the CPC Regulation. Furthermore, beyond the legal framework, there are numerous other factors that impact competitiveness vis-à-vis non-EU traders, such as differences in wages, taxation, access to investments, energy prices, infrastructure etc.

Concerning the broader impact of the legislative approach taken in the three Directives on competitiveness and innovation, traders and trade associations highlighted in the consultations the importance of striking a balance between principle-based rules and more prescriptive rules in order to ensure that businesses can innovate in their B2C sales and marketing activities. In their current form, the **Directives were perceived as being fairly balanced**; however, traders expressed **concerns about recent regulatory trends towards developing overly prescriptive obligations** about what their websites and apps should look like. For example, during the legislative negotiation on the 2023 DMFSD revision, which amended the CRD, the co-legislators introduced a mandatory withdrawal functionality (i.e. button), so consumers could withdraw from online contracts more easily. Similar approaches were also developed in Germany and France in their recent contract law revisions, with different degrees of prescriptive detail. Traders stressed the importance of allowing space for innovation in the design of their interfaces – they consider that while the law can establish the objective, they should have reasonable freedom in how to comply.

4.1.1.3. *Legal uncertainty and limitations*

Legal uncertainty

A key challenge to effectiveness concerns **legal uncertainty as regards the application of the three Directives in the digital area, in particular to new technologies and data-driven practices.** In order for the Directives to be effectively applied, monitored and enforced, there needs to be a necessary minimum of common comprehension about the existing rules by all market participants. In the public consultation, 52% of stakeholders considered that there are some legal gaps and/or uncertainties in the existing EU consumer laws in the digital area, which was supported by examples from numerous position papers. In the broader consultations and data collection, there was a consensus among the stakeholders that there needs to be more uniform legislation across the EU for consumer protection in the digital area, as illustrated by the responses to the public consultation (54% strongly agree, 29% agree).

Traders responding to the representative business survey were more positive about the state of the legal framework, with 66% of traders indicating that the current legal obligations applicable to them are clear and a further 32% indicated that they are somewhat clear. The most positive responses came from Swedish and French traders with 87% and 83% respectively indicating that the legal obligations are clear, while just 48% of Portuguese traders felt the same. When questioned about the areas of their business activities that entail legal uncertainty, the traders pointed towards the online sale of goods (64%), advertising (including personalised advertising) (18%), design of online interfaces (16%) and burden of proof in case of dispute

with consumers (16%). It is notable that the **degree of legal uncertainty about rules applicable to the online sale of goods was higher for smaller traders** (76% for traders with 1-5 people) than for larger traders (44% in traders with 55-250 employees).

There is also a perception of **legal uncertainty stemming not only from the text of the Directives but from their interpretation at Member State level**. In the targeted survey, 66% of respondents considered there to be divergences from a moderate to a great extent in the national interpretation of EU consumer law across different Member States and 49% also considered there to be divergencies in national interpretation between different competent bodies in the same Member State. This creates unnecessary costs for businesses that could be overcome by further harmonisation at EU level through legal amendments and guidelines.

Several examples of legal uncertainty are outlined in Annex VI in relation to how the Directives apply to specific problematic practices. As a cross-cutting example, there are diverging interpretations of the legal concept of a consumer's 'transactional decision' that underpins the material scope of the UCPD. In the attention economy, traders are not only focusing on getting consumers to make purchases, but also aim to keep their attention and increase engagement while using their digital services. Accordingly, in 2021 the Commission clarified in the UCPD Guidance that the concept of a transactional decision should be understood as not only covering direct purchasing decisions but also other relevant decisions about continuing to use the service, such as scrolling or viewing ads, which are particularly pertinent as regards digital services. However, for example, the Federal Supreme Court of Germany has set tighter boundaries to transactional decisions in its case law, excluding decisions such as taking a closer look at an offer in an advertisement or tapping on a social media post that has tagged a trader. Without clarity about the kinds of transactional decisions that the UCPD applies to, its ability to effectively address all types of problematic practices, such as attention-capture dark patterns, will be significantly undermined.

Despite the benefits of a principle-based approach, the **broadly worded legal provisions in the Directives might sometimes lack the necessary concreteness for their effective practical application to commercial practices and system architectures in the digital environment**. It is difficult for traders to translate these general principles into concrete development decisions in design interfaces, software, hardware, infrastructure etc. Furthermore, **general principles do not lend themselves easily to the use of technology in enforcement** (e.g. automated compliance checks through webcrawlers and other applications), in comparison to more concrete prohibitions in blacklists.

Standard of consumer behaviour

The effectiveness of the Directives is also impacted by the limitations of the core legal concepts underpinning the framework, including in particular the legal standard of the 'consumer'. The UCPD is based on the idea that, whilst it is appropriate to protect all types of consumers from unfair commercial practices, consumers who qualify as 'vulnerable' should be ensured a higher level of protection than the 'average consumer'. Increasingly, large segments of the EU population are considering themselves to be vulnerable - in the 2019 CCS, 43% of consumers surveyed believed themselves to be vulnerable consumers due to socio-demographic factors such as age, health problems, poor financial circumstance and other personal issues (up by 8 percentage points compared to 2016).[107] A recurring criticism of EU consumer law in this context is that the legal definition of the 'average consumer' is not in tune with the realities of the disengaged consumer behaviour in the digital environment and that the 'vulnerable

[107] This is reinforced by findings from other consumer reports, academic literature, and feedback from stakeholders consulted which highlighted the growth in consumer vulnerability as partly attributable to the evolving digital landscape.

consumer' definition remains too rigid and narrow, only reflecting a small number of traditionally vulnerable consumer groups. The concept of vulnerability is also criticised for focusing on the inherent weaknesses of particular groups as a fixed characteristic. Consumer organisations and several Member State respondents consider that EU consumer law fails to address a broader power imbalance - digital asymmetry - which can make all consumers vulnerable in the digital environment, with limited or non-existent bargaining power, aggravated by insufficient digital literacy, cognitive biases, information overload, manipulative design of online choice architectures, a lack of interoperability between services, among other factors.[108] In the public consultation, 51% of stakeholders called for adapting the legal benchmarks of an 'average consumer' or 'vulnerable consumer' to better reflect the real behaviours of consumers in the digital environment.

The **'average consumer'** concept, as developed by the Court of Justice and eventually codified in the UCPD but also used in other consumer legislation, refers to a person who is reasonably well informed and reasonably observant and circumspect. It is broadly considered to reflect the image of a *homo economicus* from neoclassical economic theory, which has its limitations as a benchmark for assessing human behaviour. This concept was codified in the UCPD in order to give national authorities and courts common criteria to enhance legal certainty and reduce the possibility of divergent assessments. Thus, it became an important benchmark in assessing whether a certain commercial practice is unfair or not (as indicated in Recital 18 and Articles 5 to 9 UCPD). National authorities and courts must use the average consumer benchmark when assessing a commercial practice. Nevertheless, to determine whether a practice is liable to impact the average consumer, national enforcers do not have to commission expert reports or consumer research polls, but to exercise their own judgment by taking into account the general presumed consumers' expectations. In the UCPD Guidance, the Commission expressly encouraged enforcement bodies to take insights from behavioural economics[109] into account when applying the UCPD.[110] The 2017 Fitness Check noted that this benchmark established a high standard that changed consumer protection in some Member States that previously applied more lenient threshold that took into account the possible carelessness or superficial approach of an average consumer. The 2017 Fitness Check noted that, in practice, the benchmark allows for a significant degree of flexibility in its application, while also leaving ambiguity as to how a court or authority may interpret it in a specific case.[111]

The findings of the present Fitness Check suggest that the **growing mismatch between the normative abstraction of the 'average consumer' and the realities of consumer behaviour in the digital environment** undermines the effectiveness of EU consumer law. Consumers have limited comprehension about digital commercial practices, such as the functioning of the data collection ecosystem and algorithmic processes, coupled with their limited bargaining power and the constant exposure to information overload and dark patterns that target their

[108] A 2021 study commissioned by BEUC describes digital vulnerability as a universal state of defencelessness and susceptibility to the exploitation of power imbalances that are the result of increasing automation of commerce, datafied consumer-seller relations and the very architecture of digital marketplaces.

[109] There is extensive scientific literature on cognitive biases and how commercial practices play on persuasion to influence consumer behaviour in digital environments, e.g. concept of attention deficit (Kahneman & Tversky, 1973); persuasion activating an emotional load guiding consumer choice (affect heuristic) (Slovic & Peters, 2006); persuasion inducing a misperception of risks (probability neglect) (Sunstein, 2003); six persuasion techniques identified by Cialdini (2009) - reciprocity (consumer's motivation to repay generous or helpful actions), scarcity (items becoming more valuable if less is available), authority (the use of advice from an authority figure), commitment (the need of consumers to be consistent with prior commitments), social pressure (the fact that consumers determine what is correct or acceptable based on what others do or think), and likeability (decisions being more easily influenced by someone to whom a consumer is favourably disposed).

[110] UCPD Guidance, section 2.8.

[111] Despite strong support by consumer organisations (70%) and public authorities (68%) in favour of revising the concept at the time, the Commission did not put forth a proposal for legislative changes based on the overall conclusion that there were no major problems reported in practice.

behavioural biases. Consumers have adapted to this environment by paying less attention, agreeing to contract terms without reading them and accepting 'all cookies' against their own preference. Contrary to the premise underlying the average consumer standard, they are generally not in a position to bargain with the trader or to negotiate any terms. The question about the role of behavioural insights is also the subject of a request for a pending preliminary ruling in case C-646/22.

The **'vulnerable consumer'** concept, also found in the UCPD, refers to a person who is particularly vulnerable because of characteristics 'such as' their mental or physical infirmity, age or credulity (Recital 19 UCPD).[112] The UCPD or other EU consumer laws do not define the 'vulnerable consumer' but indicate some characteristics that shape the concept of vulnerability. In the UCPD Guidance, the Commission took the position 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. The Commission's study on vulnerability defined the vulnerable consumer as one who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation or market environment, is at higher risk of experiencing negative outcomes in the market, has limited ability to maximise their well-being, has difficulty in obtaining or assimilating information, is less able to buy, choose or access suitable products, or is more susceptible to certain marketing practices.[113] When applying the concept in the digital context, the Commission considered in the UCPD Guidance that it should 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, preferences, psychological profile and mood.

However, several stakeholders consulted doubt whether this interpretation in a non-binding guidance is sufficient for ensuring legal certainty and call for the codification of these aspects in the law. Moreover, it is not sufficiently clear whether vulnerabilities can also be understood as emerging from the use of certain technologies or commercial practices. Furthermore, the current definition falls short in addressing vulnerable consumers that are at risk of discrimination, exclusion or being harassed or targeted (including by way of biases and stereotypes), for instance due to their racial or ethnic origin, gender, sexual orientation, religion or belief. Most traders and business organisations responding to the targeted survey considered the concepts of a vulnerable and average consumer to be adequate, including as regards accessibility issues (e.g. for consumers without basic digital skills, persons with disabilities, partially sighted users), whereas consumer organisations disagreed. Moreover, despite the existing reference to 'age' as a category of vulnerability, several stakeholders and Member State respondents considered that there is **insufficient focus on the vulnerabilities of children and minors, who are active in the digital environment and often the early adopters of new digital services.**

It is unlikely that case law or enforcement actions will provide more legal certainty on this specific point. The 2017 Fitness Check showed that the vulnerable consumers provision in Art. 5(3) UCPD had a limited relevance in practice and that most national courts and enforcement authorities were reluctant to apply it. There have not been significant case law developments since then. It should also be noted that there are several additional legal requirements in Art.

[112] The CRD's Recital 34 refers to the same concept of vulnerability (without the reference to 'such as' when listing the categories of vulnerabilities) when describing the factors traders need to take into account when providing pre-contractual information. The UCTD does not explicitly mention vulnerable consumers, but the Commission considered in the UCTD Guidance that the perspective of more vulnerable consumers should be taken into account when assessing the effectiveness of remedies.

[113] 'Consumer Vulnerability across key markets in the European Union – Final Report', European Commission, London Economic, VVA Consulting and Ipsos Mori consortium, January 2026.

5(3) UCPD that presently confine its application: the consumer needs to be part of a 'clearly identifiable group' of vulnerable consumers, the practice should only target individuals within that group and the harm to those consumers must be 'reasonably foreseeable' by the trader.[114] Without legislative changes, the interpretation of vulnerability is uncertain and may contrast with the tendency to refer to specific categories of vulnerable groups in other digital EU legislation, such as the GDPR, DSA and AI Act. While the approach of referring to specific groups has been maintained, new categories of vulnerable groups have been highlighted, for example, persons living in extreme poverty and to ethnic or religious minorities in the AI Act. Furthermore, whereas the UCPD mainly applies the concept of vulnerability in the context of a specific group of consumer's perspective from which a particular practice should be assessed, the DSA and AI Act refer to vulnerability as a concrete legal element in a prohibition.

Taking into account the increase of consumer reports of problematic practices over the evaluation period and the stronger potential of targeting consumer vulnerabilities at a granular level, the effectiveness of the three Directives is undermined by the increasing disparity between the consumer behaviour anticipated by the law and the realities that consumers face in the digital environment. The provisions on the 'average consumer' and the 'vulnerable consumer' may need to be further clarified or amended to ensure their effectiveness in the digital context.[115]

4.1.1.4. *Enforcement*

Insufficient enforcement

The Fitness Check indicates that the effectiveness of the three Directives is undermined by sub-optimal private and public enforcement, in line with findings from previous evaluations. During the evaluation period, there has **not been a sufficient level of case law and enforcement actions applying the Directives to digital practices, especially to novel and data-driven practices**. This problem is likely to worsen under the conditions of legal uncertainty, which has a chilling effect on enforcement and increases the risks that the litigant or authority has to bear in the face of uncertain outcomes. For the purposes of this Fitness Check, the 'sufficiency' of enforcement is determined based on the volume and content of the court and enforcement actions that have relied on the three Directives in the digital context and qualitative stakeholder views. However, no specific numeric targets are established, as this would be an arbitrary exercise, in particular taking into account the data limitations about the national court judgments and actions. Quantitative court data and statistics are either not available in most Member States or do not provide a sufficient level of detail that would enable to understand the legal provisions/Directives at stake or to distinguish between online and offline scenarios. Therefore, the enforcement analysis focuses on whether there have been, at minimum, a number of landmark actions against the biggest players on the market on the problematic practices identified in the Fitness Check.

Despite the frequent indications of dissatisfaction with the state of enforcement in the consultations by the majority of stakeholders, the targeted survey showed that the overall perceptions concerning the effectiveness of different enforcement and dispute resolution mechanisms regarding the three Directives in the digital environment are positive, with the highest effectiveness attributed to private enforcement mechanisms for ensuring consumer redress (69%), out-of-court dispute resolution (67%) and private enforcement by qualified

[114] The supporting study to the 2017 Fitness Check recommended to remove these requirements and to integrate a reference to vulnerabilities in the 'modulated average consumer' benchmark in Art. 5(2) of the UCPD.
[115] In principle, such clarifications or amendments would impact only consumer law and not contract law, however a clear conclusion on this aspect can only be drawn after assessing the impacts of possible measures.

entities (66%). The highest figures for 'ineffectiveness' were assigned to public enforcement by administrative authorities and court action (21%), but the overall assessment was still positive by the majority of respondents (57-58%).

The introduction of a provision in the UCPD by the Modernisation Directive allowing consumers to seek remedies for harm suffered as a result of unfair commercial practices could have a positive impact on ensuring that consumers can exercise their rights more effectively. However, as noted in the implementation report for the Modernisation Directive, it is too early to ascertain what impact this change has had. Although the rule came into application from 28 May 2022, there were many delays with its transposition into national rules.

The introduction of an EU-wide possibility of collective actions with the **Representative Actions Directive (EU) 2020/1828 has significant potential to improve the effectiveness of the three Directives in the digital environment**. Infringements in digital markets by a single trader can impact a large number of consumers at the same time. While the amount of financial detriment for each consumer may be small and discourage the consumer from launching individual actions, the overall detriment caused can amount to a mass harm situation, which should be remedied to ensure consumer protection and deterrence against non-compliance in the future. However, since its entry into application on 25 June 2023, there have not yet been any collective injunction or redress cases concerning digital practices.

Public enforcement and the CPC network

EU-level coordination of public enforcement for problematic practices in digital markets is necessary to ensure effectiveness, as such infringements can affect large amounts of consumers in a short amount of time and the administrative capacities of national authorities vary between Member States. The Directives lay down common substantive rules that enable the national authorities to coordinate their views and tackle infringements of EU consumer law with a cross-border dimension in the CPC network, as foreseen in the CPC Regulation.[116]

The CPC Regulation provides a set of harmonised rules to address infringements affecting several or most EU/EEA countries. Tackling infringements through the CPC increases the efficiency and consistency of consumer law enforcement because without it, consumer protection authorities of each country would be required to engage in numerous parallel proceedings at national level against the same trader. This would result in higher costs and could lead to different levels of consumer protection across the EU. The CPC system also provides efficiency for traders who are involved in a centralised dialogue, rather than having to deal with separate consumer authorities of potentially 27 Member States. The power of having several authorities working together translates into higher pressure on traders compared to a Member State acting alone and thus improved compliance by traders.

Digital practices are often cross-border in nature and obtain an EU dimension. During the evaluation period, the CPC coordinated actions have tackled specific practices by Tinder (2024), PayPal (2023), Whatsapp (2023), TikTok (2022), Shopify (2022), Amazon Prime (2022), Google (2023), Aliexpress and Wish (2021-2022), Parship (2021), Facebook and Twitter (2018-2019), Booking.com, Expedia and Airbnb (2018-2020). These actions resulted in commitments from traders to bring their practices in compliance with consumer protection legislation. However, given legal and resource considerations, **coordinated enforcement has had to focus on a selection of strategically deterrent cases in which the legal infringement at stake is sufficiently clear** and enabling national authorities to develop a common position between them. The coordinated actions have not dealt with all of the problematic practices

[116] This Fitness Check did not formally evaluate the CPC Regulation, given that a separate application report was prepared by the Commission in parallel. The focus of this Fitness Check is on substantive consumer law, not procedural instruments.

identified in this Fitness Check, such as various dark patterns, problems with influencer marketing, addictive design.

Digital market developments over the evaluation period have raised new enforcement challenges to the existing CPC system. These issues are examined in more detail in the 2024 application report on the CPC Regulation and its supporting study.[117] The key points relevant for the Fitness Check are briefly summarised. Firstly, the **procedures governing coordinated CPC enforcement actions are perceived by authorities as long and cumbersome**, thus not optimal for digitalised markets which evolve very fast and where illegal practices can spread faster and more easily across borders. Secondly, new technologies and business models also **require enforcement authorities to develop specialised expertise** at national level. Thirdly, there are differences in the capacity of national authorities to deal with enforcement cases due to **limited resources, differences in investigation and enforcement powers etc.** Fourthly, there are also problems with the **absence of tools to detect infringements** in online markets. Fifthly, due to difficulties experienced by CPC authorities to effectively coordinate the **imposition of fines** in the context of coordinated actions, the deterrent effect of the CPC Regulation remains limited. Finally, enforcement against **traders without establishment or assets in the EU/EEA** who target consumers residing in the EU has proven to be difficult.

In the digital context, the launch of national actions using the three Directives, the use of certain investigative and enforcement tools, and participation in EU-wide sweeps and coordinated actions have been **uneven across the Member State authorities** due to multifaceted reasons, including differences in the available capacities and resources.[118] Such factors have a major impact on the effectiveness of the Directives in practice. The available data on **resources and administrative capacities** of national authorities is limited. Many authorities are not able to provide estimates and in most cases the costs associated specifically with CPC activities are not distinguishable from general consumer protection activities, neither distinguishable per Directive and between the online or offline context. As shown in the efficiency section 4.1.3.3, similarly fragmented data emerged from the targeted survey concerning the costs for authorities for applying the three Directives in the digital environment. However, it was possible to conclude that the responding authorities did not perceive the additional enforcement costs related to the application of the three Directives specifically in the digital environment to be significant (33-50% reported no additional costs). Authorities pointed towards challenges related to the complexity of the consumer complaints, the underlying technologies used by traders in their commercial practices and the added complexity resulting from concurrent breaches of other digital and data laws regarding the same type of practices. In a statement that is likely to illustrate a general trend, one authority noted that the overall size of the available resources has not changed over the evaluation period - enforcement activities have been carried out by prioritising and re-allocating existing resources.

Enforcement priorities are determined by the Member States and summarised by the Commission in order to facilitate prioritisation of actions. In the digital area, **the problematic areas outlined in the Fitness Check are broadly aligned with those priorities**. The CPC network develops a biennial review taking stock of its activities and key market trends that might impact consumers in the future. The 2024 report points to concerns with influencer marketing, price presentations, AI chatbots and generative AI, features in video games and targeted advertising, which require more attention in the future.

[117] Report on the application of Regulation (EU) 2017/2394 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws, COM(2024) 311 final.

[118] Even the number of competent authorities can greatly differ between Member States, ranging from having one designated central authority (PL, HU) to having 58-60 authorities (ES, DE).

The abovementioned concerns about the multifaceted impediments to effective enforcement in the digital environment are being considered in the context of **ongoing reflections about the possible need to reform the CPC Regulation**. These reflections cover questions such as how to clarify the application of the Regulation to third-country traders, whether there is a need to adapt CPC procedures so that they function more effectively, how to increase the availability of e-enforcement tools, and whether any additional measures are required to ensure more consistent enforcement and effective deterrence. To determine the way ahead, the Commission is currently **carrying out impact assessment studies**, which examine the full range of options available for addressing the challenges. The Fitness Check confirms the importance of these reflections for the purposes of improving the effectiveness of the three Directives and additionally underlines the negative impact that legal uncertainty can have on enforceability of substantive law.

Enforceability of substantive law

As a complement to the assessment of the procedural rules in the CPC Regulation, the Fitness Check focused on the role of the substantive legal framework in supporting effective enforcement. In this context, the **Commission's interpretative guidelines were highly regarded** by all stakeholders in the consultations, as they help to understand and apply the laws more consistently. However, the guidelines are non-binding and new obligations or a common interpretation cannot be provided through guidelines in the absence of a specific provision in the Directives or CJEU case law. It is also not possible to measure the impact that the guidelines have had in practice, beyond opinion-based data. Solely providing additional guidelines or relying on voluntary commitments cannot be considered a viable solution to addressing all of the problems with effectiveness and coherence outlined in the Fitness Check.

The Fitness Check also examined **concrete measures** related to the legal framework that could facilitate more effective private and public enforcement and deter traders from deploying unfair practices in the digital environment, in particular the rules concerning the burden of proof and a fairness by design duty.

Burden of proof

Several stakeholders pointed to significant difficulties in proving the facts and required legal conditions that determine whether a breach of EU consumer law has taken place in relation to certain digital practices. Under Article 47 of the Charter of Fundamental Rights of the European Union, everyone whose rights and freedoms guaranteed by EU law are violated has the right to an effective remedy. According to the case law of the CJEU, **the principle of effectiveness requires Member States to ensure that the conditions for the enforcement of individual rights are not such that would make enforcement practically impossible or excessively difficult**. Burden of proof rules that require the victim to explain the internal functioning of systems characterized by a high level of complexity, opacity and autonomy (such as in the case of proprietary algorithms and AI) can make the right to compensation practically ineffective. If it is extremely difficult or prohibitively expensive to meet this burden of proof, consumers would be deprived of access to justice.

At present, the three Directives under evaluation do not contain general rules on the burden of proof but only regulate specific matters related to it.[119] The situation varies slightly per Directive. Art. 11(1) of the UCPD requires Member States to have in place adequate and effective means to combat unfair commercial practices. Recital 21 clarifies that while it is for

[119] Other relevant examples from EU consumer law include the Digital Content Directive, which places the burden of proof regarding the conformity of digital content and digital services primarily on the trader and the Sale of Goods Directive, which reverses the burden of proof for the conformity of goods.

national law to determine the burden of proof, it is appropriate to enable courts and administrative authorities to require traders to produce evidence as to the claims they have made. Art. 12(a) provides that enforcement authorities should have the power to require the trader to furnish evidence as to the accuracy of factual claims in relation to a commercial practice if, taking into account the legitimate interest of the trader and any other party to the proceedings, such a requirement appears appropriate on the basis of the circumstances of the particular case, and to consider factual claims as inaccurate if the evidence is not furnished or is deemed insufficient. The UCTD imposes on the trader the burden of proof that standard terms are individually negotiated and that its pre-contractual and contractual obligations, relating in particular to the requirement of transparency of contractual terms, have been fulfilled.[120] However, it leaves on the consumer the burden of proof regarding other key elements, such as the unfairness of the contract terms, which is mitigated by the duty for national courts to assess of their own motion whether contract terms on which the dispute is based are unfair, including to take investigative measures in order to complete the case file for the purpose of that assessment.[121] The CRD has rules on the burden of proof concerning specific matters: the trader bears the burden of proof regarding compliance with information obligations whilst the burden of proof regarding the exercise of the right of withdrawal is on the consumer.

At national level, with the exception of the areas harmonised at EU level, the burden of proving the existence of factual prerequisites of the plea generally lies with the claimant. Examples of national rules on burden of proof relating to the three Directives include the Greek UCPD transposition, which obliges the supplier accused of infringing the provisions to provide the court with evidence on the accuracy of the actual claims made concerning the commercial practice and, if this evidence is not submitted or is found inadequate, the assertions made by the claimant shall be deemed to be true. Aside from the rules on the burden of proof, there are also different national rules regarding the required standard of proof and related procedural modalities, e.g. concerning the accessibility, admissibility and value of the evidence presented.

53% of stakeholders responding to the public consultation supported shifting the burden of proof of compliance with legal requirements to the trader in complex cases, such as in case of technically complex digital services and products. Results of the targeted survey, which included traders and business organisations as half of the respondents, indicated more mixed views, with 26% strongly agreeing that the burden of proof should be placed on the trader in cases of major digital asymmetries and 30% strongly disagreeing with such a claim. Traders and business organisations expressed concerns about the challenges and costs resulting from a possible increase in the number of claims, including false claims that would be difficult to disprove.

Stakeholders such as national authorities and consumer organisations strongly considered that the burden of proof could be more fairly shared between the claimants (consumers, representative entities and enforcers) and traders in certain cases. In their view, it is difficult or practically impossible to prove the facts related to possible infringements due to opaque algorithmic processes and fast-evolving digital services and products as well as interface design. This undermines the effectiveness of the three Directives and leads to sub-optimal enforcement. Moreover, the resources needed to enforce EU consumer law may be more significant in case of complex digital services and products, compared to the offline environment. It may also be technically impossible to track down a personalised practice that was shown to a specific consumer, to show what type of data was used for that personalisation

[120] As resulting in particular from Articles 4(2) and 5 and confirmed by the Court of Justice of the European Union in the Joined Cases C-776/19 to C-782/19 *BNP Paribas Personal Finance SA*, paragraphs 83-89.
[121] As resulting from Articles 6(1) and 7(1) as confirmed by the Court of Justice of the European Union e.g. in case C-807/19 *DSK Bank*, paragraphs 48-54.

or to identify a specific transactional decision for legal examination when the commercial practices in question could take place over an extended period of time.

Respondents to the consultations did not call for a full reversal of the burden of proof, but rather an **easing of the burden of proof regarding the legal elements that determine the compliance with EU consumer law in complex cases**.[122] In case there were to be indicators pointing at the possibility of a breach of EU consumer law, the onus could be on the trader to provide meaningful evidence and explanations about the practice in question (e.g. to explain how the algorithm functioned in a specific case or why their website or app produced a certain outcome). If the trader did not provide such evidence and explanations, then it could lead to a rebuttable presumption that the practice was unfair. These potential consequences could **incentivise the trader, *ex ante,*** to ensure more transparency in the development of its B2C digital products and services, to document relevant evidence about its commercial practices and to take steps to ensure that other traders whose services they rely on (e.g. for production or for the design of parts of their interfaces) are legally compliant. The importance of technical documentation is also emphasised in the text on AI Act agreed by co-legislators, in particular as regards high-risk AI systems and general-purpose AI models.

Fairness by design

As an additional approach to ensuring effective implementation, several stakeholders considered that EU consumer law is also undermined by the **absence of a positive duty to trade fairly** (as opposed to the negative duty to not trade unfairly), which could include an obligation to ensure that consumer protection considerations are taken into account by design and by default. There were suggestions to **introduce a 'fairness by design' duty for traders, which would entail taking technical and organisational measures to incorporate consumer protection considerations at all stages of the product or service development**. The scope of such a duty would cover the consumer's transactional journey, from the advertising to the aftersales stage. The closest concept to this duty in EU consumer law is the existing standard of 'professional diligence' required by the UCPD, which is defined as 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. Several stakeholders considered the concept of professional diligence to be too vague to be operational in its current form. In the public consultation, 53% of respondents called for the further clarification of this concept in the digital context. Case law and enforcement actions interpreting this concept have been limited. In the UCPD Guidance, the Commission considered that online platforms should take appropriate measures to enable traders to comply with EU consumer law requirements, as a result of their professional diligence obligation.[123] The Commission also highlighted the relevance of professional diligence in the context of assessing dark patterns and data-driven personalisation practices that impact vulnerabilities. However, there is uncertainty as to the meaning of professional diligence in the

[122] Parallels can also be drawn to the revision of the Product Liability Directive (Art. 9-10) and the proposed AI Liability Directive (Art. 3-4), which addressed concerns similar to those raised in this Fitness Check. Under the proposed rules, courts would be empowered to request the defendant to provide necessary and proportionate evidence regarding the claim for compensation. The defendant's failure to comply with an obligation to disclose evidence could lead to a rebuttable presumption that the relevant legal elements have been proven, such as the defectiveness of the product in the PLD or the non-compliance with the duty of care in the AI Liability Directive. To initiate this process, the claimant would have had to demonstrate on the basis of sufficient evidence that their claim is plausible but still face, in the case of the PLD, 'excessive difficulties, due to technical or scientific complexity' in proving all of the necessary legal elements. Technical or scientific complexity would be determined by national courts on a case-by-case basis, taking into account various factors such as the complex nature of the product or technology used, such as machine learning, the complex nature of the information and data to be analysed and the complex nature of the causal link, such as a link that would require to explain the inner workings of an AI system. The defendant would have the possibility to contest the existence of excessive difficulties.

[123] Subsequently codified in the DSA Art. 31 for online marketplaces.

digital context and several stakeholders call for the concretisation of this benchmark in order to increase its effectiveness.

The business survey explored whether traders are already taking any measures similar to a 'fairness by design' duty and estimated the magnitude of such costs. 87% of traders (869 respondents), which includes mostly SMEs, indicated having taken specific measures to ensure that the online interface of their website or app is fair, user-friendly and transparent.[124]

Other EU legislation includes examples of similar approaches. The GDPR's Art. 25 requires data protection by design and default, which obligates the controller to implement appropriate technical and organisational measures and, by default, to only process personal data which are necessary for each specific purpose of the processing. Meanwhile, the DMA requires that designated gatekeepers obtain end-user consent within the meaning of the GDPR, prior to combining or cross-using personal data between their core platform services and any other gatekeeper or third-party services (Article 5(2)). The DMA's anti-circumvention rules (Article 13(4)) also prohibit the use of behavioural techniques or interface design by designated gatekeepers to undermine compliance with any of its obligations, including those that are consumer-facing. The DSA provisions on compliance by design duty (Art. 31) require online platforms that facilitate the conclusion of contracts with consumers (i.e. online marketplaces) to design and organise their online interfaces in a way that enables traders (i.e. sellers) to comply specifically with their obligations regarding pre-contractual information, compliance and product safety information under applicable EU law. In addition, the DSA mandates specific conditions for complaint-handling concerning illegal content (e.g. notices about a lack of disclosure on sponsored content, flagging fake or unsafe products), but this does not extend to other type of problems that consumers could face, such as product returns. The effectiveness of these provisions of other laws was not evaluated in this Fitness Check.

4.1.2. Coherence

4.1.2.1.*Internal coherence*

The Fitness Check identified limited evidence of internal incoherence inside or between the three Directives concerning their application in the digital environment. The rules are generally considered to be **complementary, consistent and mutually reinforcing while covering the key points of the consumer's transactional decision from the advertising, pre-contract, sales/contract conclusion, contract performance and after-sales stages**. The amendments introduced by the MD had addressed several internal coherence issues flagged in the previous 2017 Fitness Check. In the targeted survey, 64% of respondents considered that there remained incoherencies only 'to a small extent' or 'not at all' in the digital context.

It should be noted that the revision and repeal of the DMFSD introduced, within the CRD, Article 16e that prohibits dark patterns when concluding financial services contracts at a distance, while also leaving Member States the choice to adopt specific measures to address at least one of the three dark patterns listed in the provision. It also allowed Member States to maintain or introduce more stringent protection regarding dark patterns in this area. This new provision is meant to be without prejudice to the UCPD, while taking into account that the UCPD expressly allows Member States to adopt more restrictive or prescriptive requirements

[124] When estimating the resources invested into the initial implementation of the measures, 44% indicated that 1-2 employees worked on such measures. Larger traders replied that they had dedicated more resources, with 64% of traders with 250+ employees indicating they had dedicated 5 or more employees. The recurring annual costs were similar, with 52% of traders indicating that they have 1-2 employees working on it, with 37% of traders dedicating in total between 11 and 20 person-days to these activities. If external experts were used (e.g. lawyer, consultant, auditor, IT specialist), the average annual costs for 25% of traders were EUR 1000 or less and for 35% of traders between EUR 1001-2000.

for financial services (Art. 3(9) UCPD). As regards Member States that will use the available option of not transposing all the practices listed in the DMFSD, the provisions under the UCPD will still continue to apply, subject to a case-by-case assessment.

4.1.2.2.*External coherence*

With regard to external coherence with other EU legislation in the digital area, certain overlaps and complementarities can be identified. This section will outline general comments on coherence identified in the Fitness Check. Additional information about coherence is presented when discussing specific problematic practices in Annex VI.

The evaluation period saw a comprehensive overhaul of the regulatory framework on digital markets and technologies. EU legislation already applicable to or under negotiation as regards B2C relations in the digital environment includes, for example, the e-Commerce Directive, DSA, DMA, Data Act, AI Act, GDPR, ePrivacy Directive, AVMSD, Data Governance Act, P2B Regulation, Geoblocking Regulation, Product Liability Directive and AI Liability Directive. This **new legislation - despite important differences in scope and nature - will undoubtedly have implications for consumer protection**. However, given the early stage of application of most of the above-mentioned legislation, their likely impact cannot be assessed yet and this Fitness Check is not intended to evaluate the effects of these laws beyond their interaction with the three consumer protection Directives under assessment. This preliminary analysis can only examine the content of the legal text and its foreseen enforcement structures.

The Fitness Check did not identify problems between the objectives of the three Directives and other EU legislation. The **general relationship between these laws and EU consumer law is complementary**, with several laws explicitly stating that they are 'without prejudice to' consumer law (e.g. Article 2(4)(f) of the DSA, Recital 12 of the DMA, Article 1(9) of the Data Act, Article 2(9) of the AI Act). Aside from the DSA[125], consumer protection considerations are not a central objective of these laws and, accordingly, they only occasionally refer explicitly to consumer interests and harms. The most recent additions to this body of legislation primarily introduce new obligations and prohibitions for certain traders or technologies, and grant consumers individual rights and remedies.

Consumer protection reinforcements (DSA, DMA, Data Act, AI Act)

The most recent additions to the EU's digital legal framework, namely the DSA, DMA, Data Act and AI Act, introduce new provisions of particular relevance for consumer protection in the digital environment, which interplay directly with the provisions of the three Directives under evaluation. The main provisions are summarised below (in addition to a list of provisions provided in Annex VII). As explained in the problem analysis in Annex VI, this new legislation **only partially addresses some of the problematic practices examined in the Fitness Check**.

Digital Services Act

The DSA introduces additional obligations for providers of information society services, including in particular online platforms. The general exemption from liability for online intermediation service providers that host illegal content (illegal content includes also content infringing consumer protection requirements, e.g. fake consumer reviews) is maintained (Article 6).[126] The mechanisms for the removal of illegal content are reinforced and

[125] For example, as an exception, Article 1(1) of the DSA expressly refers to consumer protection as an aim of the Regulation.
[126] Article 6(3) DSA clarifies that the exemption shall not apply with respect to consumer protection law in situations where an online platform that enables consumers to conclude distance contracts with traders (online marketplace) presents information

intermediaries are liable for any damages suffered by the recipients of the service caused by infringing the obligations stemming from the DSA (e.g. not acting upon notices) (Article 54). The DSA also introduces new requirements regarding T&Cs for intermediaries, VLOPs and VLOSEs, including on certain aspects related to their transparency and better comprehension by consumers (Article 14). When the intermediary service is mainly directed at minors, then the T&Cs should be explained in a way that is understandable for them. Furthermore, VLOPs and VLOSEs also have to provide a T&C summary. The DSA prohibits online platforms from using dark patterns to distort the decisions of the recipients of the service (Article 25), except for practices covered by the UCPD and GDPR. The DSA improves the transparency of advertising[127], including by requiring the publication of an ad repository (Article 39) and requiring prominent ad labels, information about on whose behalf the ad is presented and the main parameters for targeting recipients (Article 26). Furthermore, targeted advertising is not allowed towards minors (Article 28(2)) or on the basis of sensitive data, as defined in the GDPR (Article 26(3)). The DSA also requires online platforms to put in place appropriate and proportionate measures to ensure a safe service for minors. Online platforms also need to provide for a functionality allowing users (such as influencers) to declare whether the content they provide contains commercial communications. The DSA also requires online platforms to inform about the main parameters of recommender systems (Article 27), and VLOPs and VLOSEs need to provide at least one option for each of their recommender systems that is not based on profiling (Article 38). Online marketplaces have to request the credentials of the retailers before they list them and to provide relevant information to consumers (Article 30). The DSA also requires online marketplaces to design and organise their online interface in a way enabling their online retailers to comply with their obligations regarding pre-contractual information as well as compliance and product safety information (Article 31).

Importantly, beyond the specific provisions listed above, the DSA provides the opportunity to tackle any other systemic risks to consumer protection in the context of the risk assessments and risk mitigation measures required from VLOPs and VLOSEs (Articles 34 and 35), which could also cover topics such as addictive design. The DSA also foresees standardisation in areas such as advertising transparency (Article 44) and the development of codes of conduct (Articles 45 and 46).

Digital Markets Act

The DMA establishes a list of directly applicable obligations and prohibitions regarding practices by gatekeepers that are always considered to limit contestability or to be unfair (Article 5). Gatekeepers are not allowed to process (for the purpose of online advertising) or combine personal data without the consumer's consent (Article 5(2)). It should be possible for business users to offer consumers different prices and conditions when selling products or services through their own website compared to when selling them on a gatekeeper's intermediation platform (Article 5(3)). Consumers should also be able to receive commercial communications and conclude contracts with traders outside of the gatekeeper's core platform services (Article 5(4)). Consumers should be able to access and use content, subscriptions, features or other items acquired without using a gatekeeper's services whilst using the software application of a trader through the gatekeeper's core platform services such as an app store

or otherwise enables the transaction in a way that would lead an average consumer to believe that such information or the product/service is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.

[127] As the definition of 'advertising' in the DSA is conditional on direct remuneration to the platform, the DSA's advertising provisions are mainly aimed at native advertising that is sold by the online platform (i.e. ad banners, paid placement in search results and recommendations). Concerning marketing by social media influencers through user-generated content, the DSA's rules on the transparency of 'commercial communications' will apply.

(Article 5(5)). Gatekeepers cannot restrict the consumer's ability to raise issues of non-compliance by the gatekeeper with EU or national laws (Article 5(6)). They cannot require consumers to use an identification service, web browser, payment service or related technical services of the gatekeeper, when using a third-party service that makes use of the gatekeeper's core platform services (Article 5(7)). They also cannot require consumers to subscribe or register with further services as a condition for accessing the gatekeeper's core platform services (Article 5(8)).

The DMA establishes additional obligations and prohibitions regarding practices that could be regarded as unfair and may be further specified (Article 6). Consumers should be able to easily uninstall apps on the operating system of the gatekeeper and to change default settings on the operating system, virtual assistant or web browser of the gatekeeper (Article 6(3)). It should be possible to install and effectively use new apps and app stores by third parties, including outside a gatekeeper's app store (Article 6(4)). Gatekeepers are not allowed to self-preference their own products and services compared to similar products and services of other businesses in ranking (Article 6(5)). They also cannot restrict switching between different apps and services that are accessed using the gatekeeper's core platform services (Article 6(6)). There should also be the same interoperability with the hardware and software features of a gatekeeper's operating system and virtual assistant, as enjoyed by the gatekeeper's own services and hardware (Article 6(7)) and a right to data portability concerning data provided or generated in the context of the use of the gatekeeper's core platform services (Article 6(9)). Moreover, the conditions for terminating the gatekeeper's core platform services cannot be disproportionate or exercised with undue difficulty (Article 6(13)). The DMA also introduces an obligation for gatekeepers to provide for interoperability between their own messaging service and those of providers that introduce a reasonable request, while ensuring security and end-to-end encryption (Article 7). Finally, gatekeepers cannot circumvent the obligations in the DMA through contractual, commercial, technical or any other means, including to distort the consumer's choices and exercising of their rights (Article 13).

Data Act

The Data Act regulates data access and sharing of co-generated data from connected devices. The manufacturer has to design products and related services in a way that the user can access the data generated by their use (Article 3(1)). Users also benefit from additional pre-contractual information as to how they may access, retrieve or, where relevant, erase the data, and other relevant terms (Articles 3(2) and (3)). Users have specific data access rights, which can be made on the basis of a simple request, and the data should be made available without undue delay easily, securely, free of charge, in a machine-readable format and, where relevant and feasible, continuously and in real-time (Article 4). Furthermore, the user should be able to share such data with third parties (Article 5). Third parties that receive such data are prohibited from using that data for profiling, unless necessary for providing the service (Article 6(2)(b)) and they cannot prevent consumers from making the data available to other parties (Article 6(2)(h)). The exercise of these choices or rights cannot be made more difficult through dark patterns (Article 4(4) and Article 6(2)(a)). The Data Act also facilitates switching between data processing services (cloud providers), among others, by prescribing several technical and non-technical obligations (Article 23) and by requiring switching-related rights and obligations to be laid down in a written contract, with its minimum content prescribed (Article 25). Switching charges are gradually phased out (Article 29). Concerning smart contracts, the Data Act specifies that the provider of the contract has to ensure the existence of a mechanism allowing for its safe termination and interruption (Article 36(1)(b)), which could be relevant in case of unfair contract terms.

AI Act

The AI Act promotes human-centric and trustworthy AI, including by prohibiting specific practices that may be relevant in the B2C context, such as AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques that distort behaviour and are likely to cause significant harm (Article 5(1)(a)) and AI systems that exploit vulnerabilities based on age, disability or a specific social or economic situation of persons or a group of persons to distort their behaviour and are reasonably likely to cause significant harm (Article 5(1)(b)). The AI Act categorises specific AI systems as high risk (Article 6)[128], meaning that they would have to meet more stringent requirements, including in terms of risk management and documentation. High risk AI systems (Annex III) include for example biometric categorisation according to sensitive or protected attributes or characteristics based on inference from such factors, emotion recognition, evaluating creditworthiness of natural persons or establishing their credit score and AI systems intended to be used as a safety component of a product, including that product, or if the AI system is itself a product covered by Union harmonisation legislation in Annex II. The AI Act also provides for several information obligations, in particular obliging providers of AI systems that interact directly with natural persons to be developed in such a way that persons are informed about the fact that they are interacting with an AI system (Article 50(1)), to inform consumers when they are exposed to an emotion recognition system or a biometric categorisation system (Article 50(3)), as well as to inform consumers if they view deepfakes or text published with the purpose of informing the public on matters of public interest that the content was artificially generated or manipulated (Articles 50(4)). Furthermore, any affected person subject to a decision which is taken on the basis of the output from a high risk AI system, which produces legal effects or similarly significantly affects them, shall have the right to a clear and meaningful explanation about the role of the AI system and the main elements of the decision taken (Article 86).

Regulatory complexity

The consultation activities showed that many stakeholders consider that the proliferation of EU legislation in the digital area has **increased regulatory complexity, as the new digital legislation has to be applied in conjunction with the horizontal EU consumer laws and within parallel enforcement structures**. For example, in this context, the Commission was mandated under Article 91(1) of the DSA to report by 17 November 2025 on the way that the DSA interacts with other legal acts. The regulatory complexity is a concern even where legal texts are coherent with each other. In the public consultation, only 32% of stakeholders considered EU consumer law to be coherent with other laws, such as data protection and platform regulation. Views were more optimistic in the targeted stakeholder survey, where over 60% of respondents considered there to be at least some coherence between the three Directives and other instruments, with particularly strong coherence flagged with the ePrivacy Directive[129].

To illustrate regulatory complexity, the most common coherence issue flagged in stakeholder consultations concerns the **regulation of dark patterns in different instruments**, notably in the DSA, DMA, Data Act, AI Act and DMFSD (as amending the CRD). The deployment of dark patterns could breach multiple laws at the same time. The rapid adoption of different provisions tackling dark patterns could create coherence problems during the implementation stage when striving towards a coherent understanding of the different terms used in these provisions and the accompanying recitals, such as 'coerce', 'deceive', 'manipulate', 'subvert',

[128] Unless those systems do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making.
[129] In the B2C context, the ePrivacy Directive complements the UCPD and CRD by requiring prior consent for direct marketing and for the placing of cookies and other identifiers in their terminal equipment, except under very specific circumstances.

'impair' and 'materially distort'. Specific concerns were raised about the interplay between the UCPD and Art. 25 DSA, which prohibits online platforms from deploying dark patterns, but excludes practices 'covered by' the UCPD and GDPR. The scope of the UCPD covers nearly all B2C commercial practices in the advertising, sales or after-sales stages. Many stakeholders are unsure about the scope of the provision and consider that enforcement authorities would face risks when bringing forth actions invoking it. If left unclarified, the legal uncertainty could hinder the enforcement of both the UCPD and DSA. The range of possible interpretations in recent literature even include a conclusion that business users could now be better protected than consumers, since business users benefit from a clear prohibition of dark patterns in the DSA, whereas consumers are only protected subject to a case-by-case assessment under the UCPD.[130] Several stakeholders and Member State authorities call for additional guidance and more concrete prohibitions of dark patterns to be integrated into the UCPD blacklist, which would help delineate the boundaries of unacceptable practices more clearly. Additional interpretations regarding dark patterns emerge from the DSA's compliance by design provision, which requires online marketplaces to design their interfaces in a way that enables traders to comply with their information obligations under the UCPD, CRD and UCTD, and could be used to scrutinise dark patterns that involve hiding information. Issues related to diverging interpretations could also arise when concerns related to dark patterns are tackled through the risk assessments and mitigating measures that the DSA requires from VLOPs and VLOSEs. Similarly, additional interpretations regarding dark patterns could emerge from the AI Act in the context of the various compliance activities required from providers of high-risk AI systems or when determining whether a given practice amounts to a deployment of subliminal techniques, purposefully manipulative or deceptive techniques or an exploitation of vulnerabilities according to the specific conditions listed in Article 5(1) and (2) of the AI Act. More interpretations could also emerge from the anti-circumvention rule in the DMA, which aims to capture dark patterns that gatekeepers could employ when avoiding full compliance with the obligations under the DMA, especially given its broad scope that covers any type of behaviour, whether contractual, commercial, technical or any other nature, and extends to the structure, design, function or manner of operation of a user interface or a part thereof. Such regulatory complexity increases the risk of authorities and courts arriving at diverging interpretations concerning the same or similar types of practices.

Several ongoing examples of the parallel application of consumer law and other digital laws have already emerged in practice, such as:

- Meta's pay-or-consent business model - referring to Facebook and Instagram users' choice to either continue to use the services at no monetary cost or to opt for a paid subscription - has triggered parallel discussions among competent authorities from the perspective of consumer law (UCPD, UCTD, CRD), data protection (GDPR) and digital laws (DSA and DMA). BEUC filed complaints both under consumer law (30 November 2023)[131] and the GDPR (29 February 2024)[132] invoking infringements of different provisions regarding the same type of practices. Under the DSA, the Commission sent a request for information to Meta on 1 March 2024, including on the risk assessments related to the introduction of that subscription option.[133] Under the DMA, the Commission opened proceedings against Meta on 25 March 2024 and delivered its preliminary findings on 1 July 2024, highlighting its concerns that the measures put in

[130] H.-W. Micklitz, 'Dissolution of EU Consumer Law Through Fragmentation and Privatisation', BEUC report, Digital Fairness for Consumers, 2024, p. 115
[131] 'Chose to loose with Meta', The European Consumer Organisation (BEUC).
[132] 'The Meta Smokescreen', The European Consumer Organisation (BEUC).
[133] 'Commission sends request for information to Meta under the Digital Services Act', European Commission, Press Release 1 March 2024.

place by Meta fall short of effective compliance with their obligations under Article 5(2) DMA.[134] The CPC network launched a coordinated action against Meta on 22 July 2024 on the basis of potential breaches of the UCPD and UCTD.[135]

- Temu, an online marketplace targeting EU consumers, was designated as a VLOP under the DSA on 31 May 2024 and the Commission sent a request for information on 28 June 2024.[136] BEUC filed complaints against Temu under the DSA framework for failing to protect consumers, invoking several issues such as dark patterns, lack of clear information to consumers about sellers, circulation of unsafe products etc.[137] At the same time, national consumer protection authorities (Hungary, Ireland, Poland) and consumer organisations (German organisation vzbv obtained a cease-and-desist in 2024 concerning the practices related to presenting discounts; Italian organisation Altroconsumo) had also launched separate inquiries into Temu's practices alleging consumer law breaches, including the UCPD, CRD and PID[138].

Implementation and enforcement

Several differences of approach can also be discerned concerning the implementation and enforcement foreseen for the different laws. The three Directives primarily provide *ex post* consumer protection, with an emphasis on a case-by-case assessment, whereas instruments like the DSA and DMA regulate certain problems through *ex ante* evaluation of the practices and services, including through risk and conformity assessments. The Directives focus on regulating specific outcomes for consumers, whereas the new instruments also place an emphasis on regulating the related processes, such as the content moderation processes in the DSA or the various due diligence processes for high-risk AI systems in the AI Act. A further key distinction from consumer law is the central role of the Commission as an enforcer for the DSA and DMA, with specialised teams supervising VLOPs, VLOSEs and gatekeepers. Moreover, it is notable that the implementation of instruments like the DSA, DMA and AI Act involves to some extent engaging third parties and the companies themselves, with certain aspects of compliance assessments being delegated to online platforms, gatekeepers, providers of AI systems, auditors, vetted researchers, third parties and standardisation bodies. To varying degrees, it will be up to the **shared governance between private entities, national authorities and/or the Commission as an enforcer to give meaning to the legal concepts in those laws**, including in terms of assessing consumer protection risks that are also regulated by the three Directives. This differs from the current state of EU consumer law, where the primary role for applying and interpreting the relevant legal provisions lies with national courts and authorities that have expertise in consumer protection. Coordination measures may be taken to facilitate coherence of the various instruments. For example, the DMA provides for consultation with expert bodies, including those dedicated to consumer protection, within the context of a High Level Group.

The decisions taken within the different enforcement structures concerning consumer protection aspects may have an impact on the coherence of EU consumer law in the future. The same concerns the consumer-related information generated in the risk assessments, technical documentation, audits and other relevant evaluation processes related to the new legislation, to the extent that such information would be accessible outside of those enforcement structures.

---

[134] 'Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act', European Commission, Press Release 1 July 2024.

[135] 'Commission coordinates action by national consumer protection authorities against Meta on 'pay or consent' model', European Commission, Press Release 22 July 2024.

[136] 'Commission requests information from online marketplaces Temu and Shein on compliance with the Digital Services Act', European Commission, Press Release 28 June 2024.

[137] 'Taming Temu', The European Consumer Organisation (BEUC).

[138] Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers (OJ L 80, 18.3.1998, p. 27).

Overall, the instruments have increased the availability of information to the public that may be relevant for consumer protection purposes, such as the DMA overview of the gatekeepers' audits of their consumer profiling techniques or the DSA's ad repository, annual reports on content moderation, reports by trusted flaggers etc.

The differences in the public enforcement systems accompanying this body of legislation should be further underlined. For example, the DSA and EU consumer law each have their own public enforcement system, with DSA provisions publicly enforced only by national authorities designated as competent for enforcing the DSA and the Commission under chapter IV of the DSA, whereas provisions under EU consumer law and the e-Commerce Directive are publicly enforced by national consumer enforcement authorities, including in cross-border cases within the CPC cooperation mechanism. Both the **DSA and the CPC Regulation contain very limited provisions dealing with cooperation between the enforcement authorities designated under the relevant enforcement system and authorities outside that enforcement system.** There may be challenges in the future in ensuring coherence between the parallel enforcement structures in specific cases against the same platform concerning digital business-to-consumer commercial practices and contract terms, given the close interlinks between the respective DSA and consumer law requirements. The possibility of diverging decisions on a similar set of facts contributes to the complexity of the regulatory landscape. In contrast, the DMA is enforced by the Commission and national competent authorities may assist the Commission in its role. Given that several of these laws have not yet entered into application or have only been applied for a short amount of time, it is too early to appraise their overall effects on the enforcement of consumer law.

In the area of private enforcement, there is **convergence between the three Directives and other legislation as regards collective redress**. In addition to EU consumer law, the DSA, DMA, AI Act, Data Act, GDPR and AVMSD provisions are enforceable by qualified entities under the specific mechanism of the Representative Actions Directive when the 'collective interests of consumers' are concerned. There may be considerable scope for synergies from the complementary application of these rules in a single case against a trader for the same practices aimed at consumers. However, this has remained unexplored during the evaluation period, since there have not been any digital-related actions brought and not all of the new laws have become fully applicable yet. The obstacles to effective private enforcement are multifaceted. However, the shortcomings of the current legal framework may have a direct impact on the level of incentives for bringing such actions.

Remaining challenges

In order to better understand the scale of the 'residual' problem in digital markets from the consumer protection perspective (i.e. remaining challenges following the adoption of these new Acts), the Fitness Check outlines examples of the limitations of the scope of application of the specific provisions of the legislation.

It is important to note that the application of the new rules is limited by their material scope, addressees, risk-level determinations and other factors. By design, the new Acts are not broad consumer protection instruments and **only target the practices of certain types of traders, technologies and services**.

As a consequence, the obligations within the new Acts **are not intended to cover all problematic practices that EU consumers can face, such as general issues related to the content of marketing and advertising, price promotions, remedies and contractual matters** that are regulated by EU consumer law and national civil laws. The specific problematic practices identified in this Fitness Check are either not addressed at all (e.g.

problems related to video games such as the use of in-game currencies) or are addressed only insofar the role of platforms is concerned (e.g. personalised advertising). The new Acts are also not intended to cover all traders operating in B2C digital markets that can have a significant impact on consumers in the context of commercial transactions (e.g. non-intermediary traders).

As regards digital services, **the new obligations for online platforms in the DSA and DMA target specific behaviour in relation to defined categories of digital services**. The broader definition of 'digital services' includes a wide range of services that go beyond the DSA's scope, which is exclusively focused on 'intermediary services' and 'platforms'[139], whereas the DMA focuses on specific 'core platform services' that serve as an important gateway for business users to reach end users (e.g. in addition to intermediation services, the DMA also applies to online social networks, web browsers, operating systems, video-sharing platforms, search engines virtual assistants, online advertising services, cloud services and communication services that fall in scope of the regulation)[140]. The DSA and DMA provide for extensive new obligations that tackle many problems related in particular to large social media platforms, online marketplaces, app stores and search engines, such as TikTok, Instagram, Facebook, the Amazon store and Google Search. However, depending on the technological evolution, their exact features and subject to a case-by-case legal assessment by competent authorities, it is unsure whether a range of other digital services could fall within the scope of the new obligations. These include **various apps and software, such as individual traders' e-commerce apps, media streaming services, video games, dating apps, fitness and health apps, gambling services, newspapers, newsletters and other digital content subscriptions, educational apps, translation apps, productivity apps, IoT apps, online travel operators, etc**. Market data concerning some of these digital services was highlighted in section 3, with their collective turnover amounting to billions of euros.

Furthermore, the DSA platform obligations do not apply in cases **where the dissemination to the public of third-party content is present but only minor or ancillary to the service**[141] (e.g. comments section in online newspapers). While online intermediary services and core platform services are a vital component of the internet, they are not the only relevant digital services in B2C markets that entail risks for consumers. In the consultations for this Fitness Check, some stakeholders, in particular consumer organisations and certain Member States, questioned the justification for the narrowing of some of the useful new obligations only to online platforms, thereby leaving out other traders and digital services that may also have a significant influence on consumer behaviour. For example, they called for establishing equivalent obligations in EU consumer law that would be applicable to all traders, such as the DSA's prohibition of presenting targeted advertising towards minors or based on sensitive data.

Concerning **micro and small enterprises, they are either fully or partially exempted** from certain provisions of the DSA (Sections 3 and 4) and Data Act (Chapter II) in order to keep the regulatory burden proportionate to the size of the provider. Furthermore, while SMEs are not expressly exempted, the DMA targets large undertakings with considerable economic power that provide 'core platform services' in line with strict quantitative, and in certain cases qualitative criteria, given the gatekeepers' important role in the digital economy.[142] **99.8% of**

[139] Section 3 DSA entails 'Additional provisions applicable to providers of online platforms' and Section 4 DSA entails 'Additional provisions applicable to providers of online platforms allowing consumers to conclude distance contracts with traders'. The concepts of intermediary service and online platform are defined in Art. 3(g) and (j) DSA.
[140] Art. 1(2) DMA outlines the scope of the Regulation as applying to core platform services provided or offered by gatekeepers. The concepts of gatekeeper and core platform service are defined in Art. 2(1) and (2) DMA.
[141] As explained in the definition of online platforms in Art. 3(j) and Recital 13 DSA.
[142] See also Recital 24 DMA on the applicability to SMEs. In addition, non-captured services are subject to the general obligations under the Platform-to-Business Regulation (EU) 2019/1150.

traders operating in the EU are SMEs (out of which 99% are micro and small enterprises) and they produce almost 52% of the total value added in the EU.[143] EU consumer law applies to all of these traders whenever they target European consumers, thereby providing a common baseline of digital fairness.

As regards e-commerce, the **new obligations for online platforms/marketplaces in the DSA and the DMA do not cover direct B2C online retail markets[144]**, which remain regulated by EU consumer law and other laws. In particular, the websites and apps of individual traders are not covered by those new obligations. In 2023, cross-border e-commerce in Europe (excluding travel) accounted for EUR 237 billion. The top sellers included Ikea, H&M, Lego, Jysk, Lidl, Zara, Adidas and many others whose core service does not fall under the definition of an online platform or online marketplace.[145] According to Eurostat, in 2023, **almost twice as many traders used their own websites or apps (84.7%) rather than online marketplaces (42.9%) for their sales**. These figures have increased compared to 2017 by 1.3 and 3.2 percentage points, respectively. There remain considerable differences between Member States in this regard. For example, while over 95% of traders in Estonia sold online via their own website or apps, only 42.8% did so in Lithuania, where traders preferred to sell via online marketplaces instead (82.3%).[146] Importantly, many traders also choose to operate in both venues, with SMEs being particularly reliant on online intermediation platforms like marketplaces and app stores.[147] Nevertheless, in 2022, the **e-commerce turnover of EU traders achieved via their own websites or apps was more than 6 times higher than the turnover for sales via online marketplaces**,[148] which points to the scale of the 'residual' commercial practices that fall outside the scope of the new rules applying to platforms.

As regards AI systems, the **AI Act does not qualify most consumer-facing AI systems as high risk**, which would largely leave them governed by transparency requirements and EU consumer law or other laws. This concerns AI systems such as **virtual assistants, AI chatbots (e.g. used in the context of customer service) or AI-powered toys[149]**, unless they take the form of prohibited AI practices (e.g. in case of harmful manipulation or exploitation of vulnerabilities). While it is appropriate to place the most stringent obligations on AI systems that entail the highest risk of harm to the health, safety or fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence, other types of AI systems were intended to remain regulated by EU consumer law and other laws. Moreover, **emotion-recognition AI systems** that could be used in a B2C commercial context (e.g. for the purposes of personalised advertising) were qualified as high risk but not prohibited outside of workplace and education, unless their use falls under the prohibited practices. As recognised in Recital 44 of the AI Act: *'There are serious concerns about the scientific basis*

[143] Statista, number of SMEs in the European Union 2008-2023, by size. According to Eurostat, in 2017, 13% of EU businesses reported having conducted B2C online sales. In 2022, while there was no longer a distinction provided between B2C and other sales, 22.9% of EU businesses reported making online sales and 3.1% of their total turnover came from B2C online sales (compared to 3.6% of turnover from B2B or B2government online sales).

[144] For example, the DSA does not impose obligations directly on the traders offering goods and services through online intermediaries, but rather focuses on the behaviours of those intermediaries themselves. However, the rules indirectly create conditions for traders to be present on marketplaces, and bring some rights to those traders as well, not least in terms of transparency and non-discrimination from the marketplace.

[145] Cross.border Commerce Europe, TOP 500 EU Retailers Cross-Border Analysis Report 2024.

[146] Enterprises with web sales, by type of sales, Eurostat, 2022.

[147] For example, see data from the Report from the Commission to the Council and the European Parliament, Final report on the E-commerce Sector Inquiry, COM(2017) 229 final.

[148] 'ICT usage and e-commerce in enterprises' survey, Eurostat, 2023. The survey included approx. 161 000 enterprises, with 10 or more employees or self-employed persons, out of 1.5 million in EU. Out of these 1.47 million enterprises, approximately 83 % were small enterprises (with 10-49 employees or self-employed persons), 14 % medium (50-249 employees or self-employed persons) and 3 % large enterprises (250 or more employees or self-employed persons).

[149] Assessment on a case-by-case basis is required, for example AI-powered toys could qualify as 'high risk' if the AI system is a safety component and the toy is subject to third party conformity assessment.

of AI systems aiming to identify or infer emotions (…) Among the key shortcomings of such technologies, are the limited reliability' (emotion categories are neither reliably expressed through nor unequivocally associated with a common set of physical or physiological movements), *'the lack of specificity'* (physical or physiological expressions do not perfectly match emotion categories*) 'and the limited generalisability'* (the effects of context and culture are not sufficiently considered). Such concerns are also present in the context of the use of emotion recognition in B2C relationships (i.e. retail, e-commerce, advertising, customer service), especially concerning the potential misuse of such technologies to unduly influence consumer decision-making,[150] and remain relevant under EU consumer law. Regarding the future-proofness of the AI Act, the Commission will have to undertake annual review of the list of the high-risk use cases in Annex III and the prohibitions which will allow to include other use cases if evidence arise justifying their inclusion.

Despite the above delineation of examples of remaining challenges that fall outside of the scope of the new Acts, there are nevertheless potential **overlaps and grey areas concerning the parallel application of EU consumer law in conjunction with other digital laws concerning similar or exactly the same commercial practices by the same traders**. The **potential measures that could be taken in the interim** to address regulatory complexity and ensure a strong, consistent and coherent application are presented in section 5 on conclusions and lessons learned.

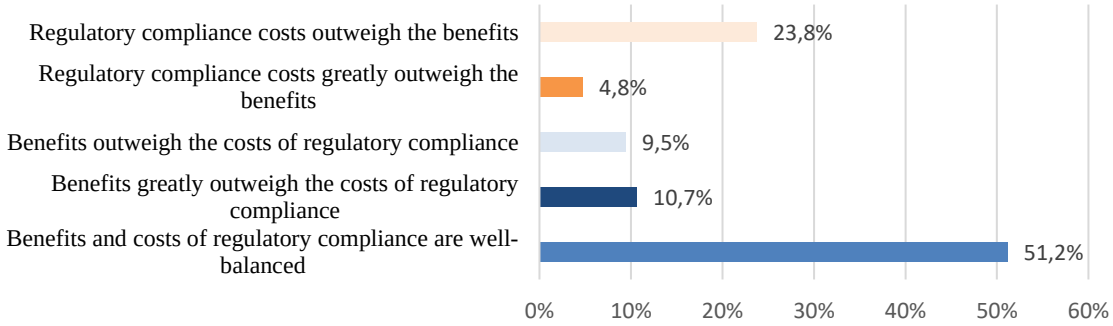
4.1.3. Efficiency

The Fitness Check carried out a **partial cost-benefit analysis** associated with applying the three Directives in the digital environment, subject to certain limitations. The **benefits were assessed only in a qualitative manner**, whereas the costs for businesses were quantified. The main challenge with quantification concerned the isolation of business costs specifically in relation to digital practices, as the interventions cover both online and offline environments. Multi-channel traders find it difficult to disentangle compliance costs associated with digital channels from offline channels and most traders are unable to isolate costs for the three Directives specifically. The estimates given by traders are also likely to include national legislation going beyond EU consumer law requirements as well as certain EU sector-specific legislation and its national implementing legislation.

Overall, based on the consultations, to the extent that the costs and benefits are quantifiable and attributable, the costs associated with the application of the three Directives in the digital environment can be considered proportionate to the benefits, with limited simplification potential identified. In the targeted stakeholder survey, which included all key stakeholders (i.e. EU-level trade associations, consumer organisations, Member State representatives), 51% of respondents found the costs to be well-balanced, while 24% considered the regulatory compliance costs (i.e. all costs associated with the application of the three Directives) to outweigh the benefits.

[150] For example, in 2022 the Hungarian data protection authority issued its highest fine to date concerning the use of AI by a Hungarian bank to analyse voice recordings of customer service calls to predict the consumers' emotions and such information was used to rank the follow-up calls in order of priority. The decision considered that, among other issues, there was not a sufficient impact assessment and balancing test documentation in compliance with the GDPR.

Figure 6 - Stakeholder perceptions of the costs and benefits of the Directives in the digital environment at a societal level[151]



Source: Targeted stakeholder survey to support the Fitness Check

The following sections will expand on the costs and benefits with more granularity.

4.1.3.1. *Business benefits and costs*

Overview of benefits

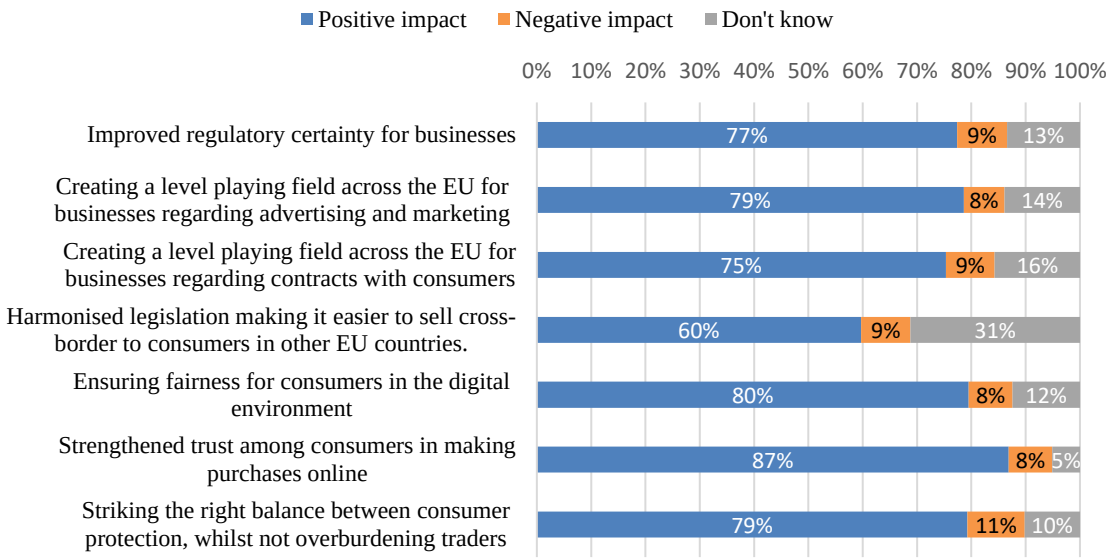
The business survey explored the potential benefits related to the existing EU-level harmonisation of rules concerning advertising and standard contract terms in the digital area. The majority of traders noted a positive impact for each of the listed categories of benefits: strengthened consumer trust in making purchases online (87%), ensuring fairness for consumers in the digital environment (80%), striking the right balance between consumer protection whilst not overburdening traders (79%), creating a level playing field across the EU as regards advertising and marketing (79%) and B2C contracts (75%), improving regulatory certainty for businesses (77%) and harmonising legislation to make it easier to sell cross-border (60%). As explained earlier in the 'effectiveness' section in the context of impacts on competitiveness and innovation, securing a high level of consumer protection and trust are necessary preconditions for fair growth. As 77% of the respondents to the business survey were SMEs, it can be deduced that most SMEs perceive that EU-level harmonisation through the three Directives has led to positive impacts that greatly outweigh the negative impacts.[152]

The area in which the largest number of businesses indicated a negative impact concerned striking the right balance between consumer protection and not overburdening traders, although the figure for the negative impact was still very low at 11%. The largest proportion indicating a negative impact in this area were companies with 50-250 employees (19%) and companies from France (18%).

[151] "At the societal level, to what extent do the provisions of the three EU consumer law Directives (i.e. CRD, UCTD, UCPD) achieve an adequate balance between regulatory costs for traders and benefits for consumers and other stakeholders?" (n=84)

[152] About 78.5% companies with 1-9 employees, 75% of companies with 10-49 employees and 52% of companies with 50-250 employees and 81% with more than 250 employees considered that the harmonisation improved regulatory certainty for business. About 60.5% companies with 1-9 employees, 56% of companies with 10-49 employees, and 52% of companies with 50-250 employees and 61% with more than 250 employees considered that the harmonisation made it easier to sell cross-border to consumers. About 82% companies with 1-9 employees, 71% of companies with 10-49 employees, and 91% of companies with 50-250 employees and 88% with more than 250 employees considered that the harmonisation strengthened trust among consumers in making purchases of goods and services. About 79.5% companies with 1-9 employees, 76% of companies with 10-49 employees, 73% of companies with 50-250 employees and 82% with more than 250 employees considered that the harmonisation struck the right balance between consumer protection while not overburdening industry.

Figure 7 - Business perceptions of the benefits stemming from the application of the Directives in the digital environment[153]



Source: Business survey to support the Fitness Check

The Fitness Check focused on the benefits for consumers when they act as online purchasers since the three Directives aim at protecting them as the weaker party vis-à-vis traders. The CJEU has constantly held that, under the EU consumer acquis, a relation between two traders is not characterised by the same imbalance that is present between the consumer and its trader and justifies particular protection for consumers (e.g. Case C-173/23 Eventmedia Soluciones). Nevertheless, traders can also indirectly benefit from the application of consumer law in the digital environment. In particular SMEs may use the same online shopping interfaces as consumers for acquiring supplies for their business activity and thus benefit from the consumer law requirements regarding transparency of the information and fairness.

Costs related to the Directives

Before presenting the findings on costs, some relevant considerations must be provided. Traders that face compliance costs with EU consumer law in the digital environment include sellers engaging in e-commerce, online marketplaces, online platforms as well as new types of traders, such as professional social media influencers. The nature and degree of the costs vary between traders, especially depending on whether they engage in the online sale of physical goods, provide digital content or services, advertising, intermediation or engage in other commercial practices. For example, there is a major difference between the costs faced by a social media influencer that simply needs to add an advertising disclosure (e.g. hashtag) in a sponsored post and refrain from unfair advertising practices, in comparison to the costs of operating an e-commerce webshop that entails processing the returns of physical goods.

Another relevant consideration is that a significant part of the legal provisions under discussion do not entail any specific costs for traders - the UCPD and UCTD contain principle-based provisions, which means that they do not necessarily prescribe detailed requirements but require traders to act in accordance with principles of good faith, transparency and due diligence towards consumers. This is the type of 'common sense' behaviour that a well-intentioned trader

[153] "Please indicate if the harmonisation of rules concerning advertising/marketing and standard contract terms for online sales has had a positive or negative impact on your company." (n=1000)

would display towards consumers, regardless of the legal requirements. Similarly, in estimating the costs, a discount can be made when considering the 'business as usual' costs that traders would incur regardless of the obligations in the Directives (e.g. providing a 'buy button', providing basic information about products and services). High business as usual costs can be assumed for most traders given that most compliance costs would have been one-off, and many of the core consumer law requirements are by now well-known. As the Directives have been in place for over a decade, the initial familiarisation costs are only relevant to traders that apply EU consumer law for the first time or in case of new amendments to the Directives, e.g. by the MD or 2023 DMFSD revision.

While costs regarding some of the information disclosure requirements introduced by the MD are only faced by online platforms and marketplaces (e.g. disclosure of search ranking parameters), most information obligations apply to all traders, regardless of their business model. Moreover, there are only a limited number of digital-only provisions in the three Directives, whereas most provisions apply to both online and offline environments. Another relevant consideration is that traders have difficulties in distinguishing between the costs related to rules stemming directly from the Directives and those stemming from additional national laws, especially in the case of minimum harmonisation in the UCTD (e.g. additional costs of complying with national blacklists of unfair contract terms).

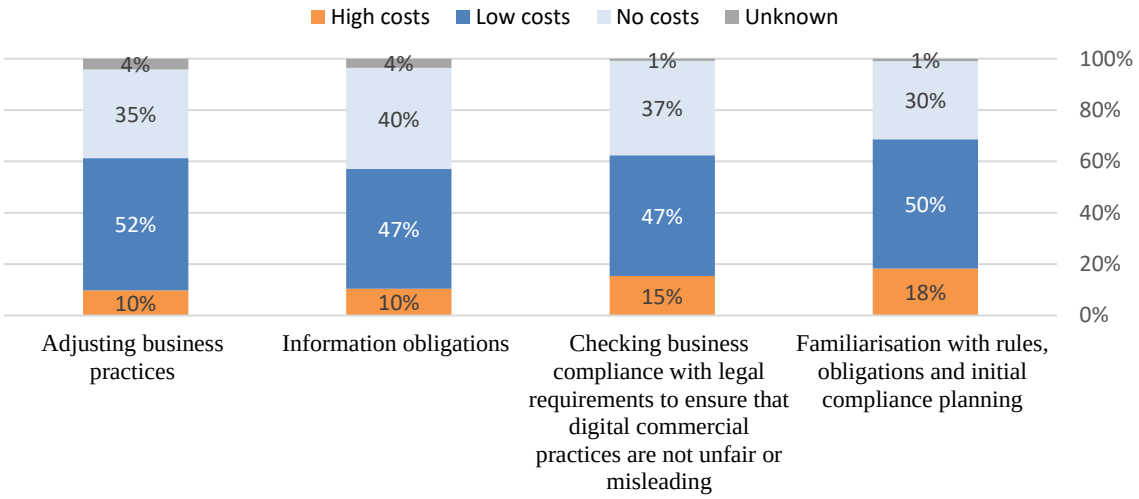
In line with the Better Regulation guidelines, the costs for traders are presented as regular and one-off adjustment costs and administrative costs. These costs stem from compliance activities such as familiarisation with rules and initial compliance planning (e.g. reviewing the applicable laws, developing compliance strategies, allocating compliance responsibilities), checking compliance with legal requirements to ensure that digital commercial practices and contract terms are not unfair (e.g. check website design or T&Cs), compliance with information obligations (e.g. ensuring the provision of pre-contractual and contractual information, disclosure requirements for platforms on search ranking and consumer reviews) and adjusting business practices (e.g. changing website design or T&Cs if unfairness is identified). Traders that operate cross-border face additional costs due to diverging national laws and differences in the implementation among Member States. Smaller companies may have to outsource some of these activities, whereas larger companies may be able to absorb these within the existing departments.

The overview of costs is based on the primary data collected in the supporting study (business survey, targeted survey, interviews, public consultation), complemented by relevant secondary data and information sources. Additional information on the cost estimations and the selection of traders/sectors is provided in Annex II and Annex V. Not all traders were able to provide quantitative responses, but it was nevertheless possible to estimate the degree of costs.[154] In general, traders had difficulties with providing quantified estimates of the costs for the individual pieces of legislation and separating the costs for online vs offline environments. Overall, for the purpose of quantifying the costs, the most robust findings stem from the business survey, which included 77% of SME respondents and found that the **costs associated with compliance with EU consumer law in the digital area are not considered high by the majority of respondents – only 10-18% of traders report high costs relating to the**

[154] Traders were specifically asked about estimations of compliance costs in the business and targeted surveys. The business survey comprised of 1000 traders in 10 Member States (FR, DE, EE, IT, ES, HU, SE, PT, PL, RO). The targeted survey received 164 responses, among which 83 responses were from individual traders and trader associations, which included approximately 24% of traders operating both online and offline, and 18% only online, and 70% of the respondents reported trading cross-border.

different compliance activities, whereas the majority face low costs or no costs at all.[155] The reasons for the low levels of costs primarily relate to the nature of the legal obligations (non-prescriptive, technology-neutral, 'common sense'), the stability of the regulatory framework over a long period of time and the absence of reporting requirements.

Figure 8 - Business perceptions of the costs associated with compliance with the Directives in the digital context[156]



Source: Business survey to support the Fitness Check

The compliance activity for which the largest number of respondents indicated high costs was **familiarisation with rules, obligations and initial compliance planning** (18%), with the highest figures from traders in Portugal (29%), Germany and Sweden (26%), and in the sector of retail sale of information and communication equipment in specialised stores (24%). When looking at the responses per type of trader, online marketplaces viewed familiarisation costs as being high the most frequently (34%), which could be related to the additional specific requirements introduced by the MD, DSA and other legislation. In contrast, only 15% of traders selling goods online through a website or app perceived the costs to be high. Overall, the adjustment and administrative costs related to applying the new changes from the MD were perceived as moderate by respondents in the targeted survey, with the highest costs (30.8%) associated with the disclosure of ranking criteria and paid ads in search, and about the processing and verification of consumer reviews.

As regards the costs for checking compliance with legal requirements, the highest costs were reported in Portugal (25%) and within the sector of retail sales of telecommunications equipment (24%). As regards adjusting business practices, 52% indicated low costs, most commonly in Spain (72%). Notably, compliance activities with regard to information obligations recorded the greatest percentage of no costs (40%), with the largest percentage of respondents facing no costs in Sweden (50%). The business survey findings differ to some extent from the open feedback during interviews and the targeted survey, as certain traders find

[155] The business survey was used for estimating costs due to its robustness. As a complementary source of information to the business survey, 80% of traders and business association respondents in the targeted survey indicated that they face additional compliance costs from the legislation from a moderate to great extent, mostly to do with familiarisation and adjusting business practices. However, the sample size was just 43 traders. The targeted survey also asked about estimations regarding the increase in the additional costs, however, the sample size was 16 traders. It is notable that most of the traders responding operate cross-border, which could explain trader perception of a higher level of compliance costs, given differences in MS implementation. For a complete overview of the data, please refer to the supporting study.

[156] "To what extent has compliance with EU consumer law requirements in the digital area resulted in the following types of costs for your business?" (n=1000)

pre-contractual information requirements burdensome, but there are likely to be differences of views in this regard between sectors and individual companies (e.g. 18% of online marketplaces and 20% of online sellers of non-digital services reported highest costs, compared to only 5% of providers of free digital services).

Additional information on the **breakdown of costs per company size** shows that smaller companies usually report the lowest costs. Regarding the costs associated with the familiarisation with the rules, around 14% of companies with 1-9 employees, 19% of companies with 10-49 employees, 23% of companies with 50-250 employees and 27% with more than 250 employees declared that they face high costs. Regarding the costs associated with the checking of business' compliance with the legal requirements, around 9.5% companies with 1-9 employees, 20% of companies with 10-49 employees, 29% of companies with 50-250 employees and 23% with more than 250 employees declared that they face high costs. Regarding the costs associated with the information obligations, around 7.5% of companies with 1-9 employees, 14% of companies with 10-49 employees, 21% of companies with 50-250 employees and 13% with more than 250 employees declared that they face high costs. Regarding the costs associated with adjusting business practices, around 6.5% of companies with 1-9 employees, 15% of companies with 10-49 employees, 17% of companies with 50-250 employees and 12% with more than 250 employees declared that they face high costs.

In order to extrapolate the business survey results to the EU level, the following calculations were carried out. Several assumptions were developed for quantification and extrapolation. The total number of possible traders affected by costs related to the three Directives in the digital environment is estimated at 1.3 million. Drawing on Eurostat and other data (e.g. Statista, impact assessment of the Digital Services Act), this figure includes online retailers engaging in B2C sales estimated at 1.254 million, in addition to approximately 10 000 traders participating in the online platform economy and 28 000 traders offering digital subscriptions, which were considered to be the main sectors relevant for B2C sales in the EU digital market that entail more significant compliance costs for businesses. The extrapolation to the EU level on the basis of the quantitative estimates from the business survey is considered sufficiently reliable, since it included all types of digital economy players, ranging from online retailers selling physical goods to traders providing digital services for 'free' in exchange for consumer data. The overall approach and assumptions for the business cost estimations were the same as in the earlier 2017 Fitness Check in order to ensure comparability to the extent possible. Although the focus of the present evaluation was on traders that provide products or services in the online environment, some sectoral continuity was ensured with the 2017 Fitness Check by including some of the same traditional sectors which engage in both online and offline sales (e.g. telecommunications).

The costs[157] are presented as a range. The higher range of costs are for traders that need to outsource compliance activities (e.g. to law firms), whereas the lower range of costs are for traders that deal with compliance in-house. Generally, **administrative costs tend to be recurrent costs, whereas adjustment costs tend to be one-off costs**. When estimating the overall volume of costs, the percentage of traders that face high costs is taken as a reference point. In terms of resources invested in **adjustment costs** related to implementing legal requirements into business procedures, a large percentage of respondents (48%) noted that between 1 and 2 employees were responsible for such adjustments, with the majority dedicating between 11 and 20 days/person. Overall, 35% of traders could not provide a cost estimate, 49% provided a cost of EUR 2000 or lower, and 16% reported greater than EUR 2000 in costs. The

[157] The compliance costs are divided into two main categories: adjustment costs (investments and expenses borne in order to adjust their activity to the requirements contained in a legal rule) and administrative costs (costs borne as a result of administrative activities performed to comply with administrative obligations included in legal rules).

average costs for companies to acquire external services was EUR 2331 and the median EUR 1600. When considering that up to 10% of traders report high adjustment costs (which amounts to 130 000 traders), at a value of EUR 1600 (based on the median), then based on the number of traders that operate online in B2C markets in the EU, the adjustment costs can be estimated at EUR 208m across the EU per year, or in case the higher average value is used that includes the costs of hiring external services (EUR 2331), then the total costs could increase to EUR 303m.

Despite the absence of reporting requirements or any other direct administrative burdens in the Directives, traders reported facing **administrative costs**. These costs are primarily related to regularly checking whether their commercial practices, advertising activities and contract terms continue to comply with legal requirements, e.g. checking whether new T&Cs do not contain unfair terms or verifying the content of new marketing campaigns or digital services. The Directives do not require traders to conduct such regular checks and the legal framework has been relatively stable over the years, but some traders nevertheless report that they are diligently verifying whether their practices are compliant, on a voluntary basis. It must be emphasised that these estimates related to regular compliance checking activities are the result of a broader compliance check that includes other legislation, such as national legislation, sectoral EU laws and national case law developments. In particular, in areas of minimum harmonisation (UCTD), it is likely that there are national case law developments that require companies to stay up to date. It is also possible that some traders are undertaking such checks in order to comply with national legislative updates, reporting or due diligence obligations. As indicated earlier, traders are unable to disentangle such costs on the basis of the origin of the laws. As a result of these combined effects, these administrative costs cannot be fully and directly attributed to the Directives. In terms of resources invested into complying with the legal requirements every year, 17% of traders checked for compliance once every six months, a further 28% once per year, 17% once a month or more often and 33% once every three months (the most popular response option). A very small percentage checked once every two years or less than once every 2 years. In the targeted survey, traders and trade associations reported checking more frequently, with 44% checking once a month or more often. Overall, 84% of companies reported low costs or no costs related to such compliance activities. In terms of the resources used annually, for those experiencing costs, the dedicated resources in terms of employees (1-2) and number of worked days were similar to those incurred in the initial implementation phase (21). The average for costs of external services annually was estimated at EUR 2547 and the median EUR 1800. When considering that up to 15% of traders report high administrative costs (which amounts to 195 000 traders), at a value of EUR 1280 (based on the median), the administrative costs can be estimated at EUR 249.8m across the EU per year, or in case the higher average value is used (EUR 2500), then the total costs could increase to EUR 487.5m.

A complete table of costs and benefits is provided in Annex IV. A summary table of the estimated business costs is provided below, extrapolated to the EU27, covering all businesses affected by costs.

Table 7 - Summary table of the estimated total annual business costs across the EU27 associated with compliance with the Directives in the digital context

Direct compliance costs	Adjustment costs (one-off) - *familiarisation with the law and initial compliance planning;*[158] - *adjusting business practices.*	EUR 208 million – 303 million

[158] Under the new BR Guidelines Toolbox (latest version July 2023), familiarisation costs are considered to be adjustment costs, p. 510.

	Administrative costs (recurring annually, not entirely attributable to the Directives) - *checking compliance with the law;* - *information costs.*	EUR 249.8 million – 487.5 million

Source: Business survey to support the Fitness Check

In comparison, the 2017 Fitness Check, which covered both online and offline environments as well as additional Directives, estimated that the total costs incurred by all businesses in the EU-28 in five selected sectors[159] for checking that their marketing and standard contract terms comply with national legislation and adjusting business practices, if needed, amounted to EUR 278 million per year. This amounted to approximately 0.024% of their turnover, of which 0.011% concerned compliance with rules concerning marketing practices and 0.009% for rules concerning standard contract terms. Those estimations were based on business interviews, including two thirds of SME respondents. When comparing the 2017 figures to the 2023 figures in this Fitness Check, the total costs are higher (EUR 278 million vs EUR 511-737.3 million), however, the scope of the 2017 figure was limited to only five sectors, whereas this Fitness Check covered all digital services and traders operating in the digital environment that engage in B2C practices. Furthermore, the 2017 estimations did not include the CRD, which is a Directive with prescriptive requirements that create additional costs for traders engaging in e-commerce, in particular, the cost of handling the return of physical goods when consumers exercise their right of withdrawal. Despite the differences in scope, these cost estimations are broadly consistent and enable to conclude that the **adjustment and administrative costs associated with EU consumer law continue to be relatively modest, in particular in the context of the revenues generated in the digital economy** (see section 3 for figures on digital market growth).

Costs from the lack of EU-level harmonisation

The Fitness Check also examined the extent of the **additional costs stemming from differences in national laws, which can arise from regulatory fragmentation**, although these costs were not precisely quantified due to the difficulty of obtaining robust data from businesses. These additional costs only concern traders that operate cross-border and can stem from the divergent application due to different interpretations related to the transposition of EU consumer law, from regulatory uncertainty and from the development of national rules going beyond or on top of the legislation. Examples of diverging national laws and implementation differences can be found in Annex VI regarding problematic practices (e.g. national rules applicable to digital subscriptions; diverging case law on influencer marketing). Subject to all the above-mentioned caveats about the impossibility to isolate the specific costs related to the three Directives at stake, there was overall **a high incidence of additional costs expressed in the business survey, targeted stakeholder survey and interviews**. This shows that the current level of harmonisation provided by EU consumer law may be insufficient in the digital environment.

When entering another Member State's market, 81% of relevant respondents to the targeted survey (traders that operate cross-border and trade associations representing them) **reported incurring additional compliance costs** regarding the rules on pre-contractual information, advertising/marketing and standard contract terms.

100% of traders and business associations responding to the targeted stakeholder survey claimed to face moderate to great costs due to differences in national legislation and

[159] For an estimated number of 962 261 businesses in the following sectors: large household appliances, electronic and ICT products, gas and electricity services, telecommunication services, pre-packaged food and detergents.

implementation, as shown in the table below. The highest costs concerned adjusting business practices (39.3%), costs of external services (33.3%), checking compliance with additional national laws (26.7%), familiarisation with national laws and initial compliance planning (25.8%) and additional information obligations (23.3%).

Table 8 - Trader and business association perceptions of the costs due to differences in national laws when trading cross-border related to practices in the digital environment[160]

Type of costs	To a great extent	To a moderate extent	To a small extent
Additional information obligations	23.3%	60.0%	16.7%
Familiarisation with national laws and initial compliance planning	25.8%	74.2%	0%
Checking compliance with additional national laws	26.7%	66.7%	6.7%
Cost of external services	33.3%	60.0%	6.7%
Adjusting business practices	39.3%	42.9%	17.9%

Source: Targeted stakeholder survey to support the Fitness Check

SMEs that responded to the business survey mostly operate only at national level, with the most active SME cross-border trading occurring in France, Germany and Austria. The overall **additional compliance costs for SMEs that trade cross-border were perceived as moderate** (with only 17% indicating high costs stemming from the familiarisation with the national legislation and initial compliance planning).

While the primary focus of this Fitness Check are the costs associated with the rights and obligations in the three Directives, regulatory fragmentation among Member States which goes beyond or on top of those rules is recognised as an issue. The solution to this problem involves ensuring more uniform interpretation as regards the grey areas and possibly more harmonisation at EU level in order to limit the possibilities for divergencies. The scale of this problem vis-à-vis specific areas and a quantification of the related costs could be further explored in the context of impact assessments for possible regulatory reforms, if necessary.

4.1.3.2.*Impacts on consumers*

The benefits of EU consumer law for consumers include enhanced consumer welfare[161] and trust in digital markets, enabled by access to clearer information and reduced exposure to unfair practices and unfair contract terms. The 2023 CCS shows that the percentage of consumers conducting online transactions increased from 57.8% in 2016 to 71% in 2022 (a 23.2 percentage point increase) and the consumer survey conducted for this Fitness Check shows that 83% of consumers made some form of online purchase or used a product or service online in 2022-2023, which confirms that consumers are increasingly actively participating in digital markets.

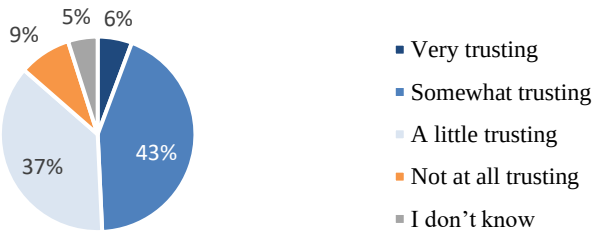
[160] "To what extent when trading cross-border has compliance with consumer law requirement resulted in the following types of costs due to differences in national transposition and interpretation?" (n=31)

[161] This Fitness Check assesses the benefits in a qualitative manner. Previous studies have attempted to quantify the increase in consumer welfare, but not specifically for the three Directives in the digital context. For example, the 2017 impact assessment for the DCD and SGD estimated a EUR 18 bn increase in consumer welfare from the harmonised rules in the form of better prices and increased choice.

Consumer trust in traders can be attributed at least partly to the development of the EU consumer law acquis over the last 50 years, including the three Directives that were adopted in the last 10-30 years as digital markets started to emerge. In the 2023 CCS, 76% of consumers agreed that, in general, retailers and service providers respect consumer rights, although trust levels vary by different demographic characteristics such as age, level of education and financial situation.[162] Younger people and those with higher levels of education tend to have higher levels of trust, while those in a difficult financial situation show less trust. The connection between consumer trust and the ability of traders to innovate was highlighted in section 4.1.1.2 on competitiveness.

In the representative consumer survey, 6% of consumers indicated that they are 'very trusting' of online businesses, whereas 43% were 'somewhat trusting' and a further 37% 'a little trusting'. Paradoxically, **despite increasing levels of digital consumer transactions, a significant proportion do not have strong trust in traders when conducting such transactions.** This indicates that there is additional scope for increasing consumer trust in the digital area.

Figure 9 - Consumer trust in online traders[163]



Source: Consumer survey to support the Fitness Check

There are **no costs for consumers** due to the application of the three Directives, however, the traders' non-compliance with the rules results in consumer detriment, which has increased over the evaluation period. Post-redress financial detriment was quantified at EUR 7.9 billion per year (see section 3 on how the situation has evolved). This detriment could also be viewed as unrealised benefits that were meant to be received from the correct application of the three Directives.

4.1.3.3. *Impacts on consumer authorities*

The benefits for consumer authorities mainly stem from the increased regulatory certainty about the applicable rules in the digital environment in areas that are harmonised at EU level. Harmonised rules also facilitate cross-border enforcement cooperation through common positions in the CPC Network and enable the exchange of best practices and information with other authorities. Furthermore, the introduction of more deterrent fines and civil remedies through the changes by the MD in the three Directives may reduce non-compliance in the future and thereby also reduce the cost of enforcement.

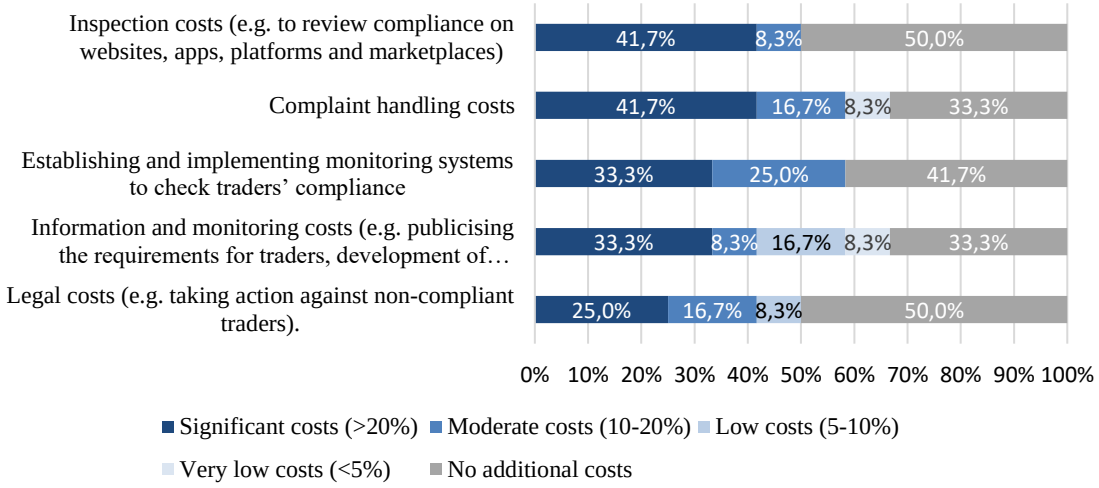
In terms of costs, in addition to the **one-off initial costs** of familiarisation with rules and subsequent amendments, the **recurring costs** related to the implementation of the three Directives for the national authorities include complaint handling costs, inspection costs (e.g.

[162] The question did not differentiate between online and offline environments.
[163] "How trusting are you of online businesses and websites?" (n=10,000)

review compliance of websites, contract terms), establishing and implementing monitoring systems to check traders' compliance, information and monitoring costs (e.g. publicising the requirements for traders, development of guidance documents) and legal costs for enforcement, including carrying out strategically deterrent cases and engaging in cross-border enforcement cooperation. The targeted survey showed that authorities do not perceive the additional enforcement costs related to the application of the three Directives specifically in the digital environment to be significant (33-50% reported no additional costs). The most significant costs relate to **inspection** and **complaint handling**; however, the responding authorities did not provide additional details on the magnitude of the costs to enable further analysis.

Most consumer authorities that responded to the survey were **not able to quantify the costs.** The costs associated with the amendments introduced by the MD, which included digital-focused provisions, were also perceived as having limited additional costs.

Figure 10 - Enforcement authorities' perceptions of the degree of additional costs when applying the Directives in the digital environment[164]



Source: Targeted stakeholder survey to support the Fitness Check

A few national authorities publish annual activity reports, which include data on resources used for enforcement activities, but it does not enable to distinguish between the resources used per national or EU legislation, per Directive or between online and offline infringements. Nevertheless, it is useful as an illustration – the 2022 activity reports show major divergence between the resources spent even among the most active and well-funded authorities in the EU. For example, the Belgian authority reported spending 237.3 Full Time Equivalents (not only for consumer law, but also certain B2B and sectoral laws), handling 51 874 complaints and processing 18 625 inspection files.[165] The French authority reported employing 2885 agents (not only for consumer law but also product safety and competition law), including 1779 investigators across central and local agencies, handling 267 300 complaints and inspecting 88 400 physical establishments and websites (around 60% of the actions concerned consumer

[164] "What have been the additional costs of the enforcement of the provisions in the three core EU consumer law Directives (i.e. CRD, UCPD, UCTD) being applied in the digital environment? Were these significant, moderate, low or did they not have any impact in your view for the following cost types." (n=16)

[165] SPF Economie, 'Rapport annuel 2022 - Direction générale de l'Inspection économique', available at : https://economie.fgov.be/fr/publications/rapport-annuel-2022-direction

protection).[166] The Swedish authority employed 177 employees, handling 26 400 complaints and closed 245 ongoing enforcement actions.[167]

Feedback from interviews and position papers points to challenges in bringing enforcement actions due to the complexity of the complaints and the underlying technologies as well as the fact that digital-related strategic deterrent cases often include concurrent breaches of other digital and data laws. The need for a broad range of expertise in digital technologies and legislation was considered to be more costly, compared to cases in the offline environment. Several authorities highlighted the need for technical expertise, forensic IT capabilities, investments and constant development of the related systems. One authority also highlighted the costs associated with possible litigation and lobbying in actions regarding large digital traders that have more resources. The challenges with enforcement have been further detailed in section 4.1.1.3.

4.1.3.4. *Scope for simplification and burden reduction*

The three Directives do not contain any reporting obligations of traders to the Commission or to the Member States. They only set out a general, normally one-off, requirement for the Member States to report to the Commission on the transposition of the Directives (including the provisions on penalties) and the use of the regulatory choices, where applicable.

The Fitness Check found **limited potential for simplification and burden reduction, specifically in the area of information requirements and the right of withdrawal**.[168] In the public consultation, a majority of stakeholders considered that there is still some scope for simplification and burden reduction (26% strongly agree and 38% agree), which was further supported in the stakeholder position papers by both trader and consumer representatives. In the targeted stakeholder survey, the majority of respondents considered there to be opportunities to simplify the legislation or to reduce unnecessary regulatory costs without undermining the objectives of the three Directives (38% to a great extent, 31% to a moderate extent, 22% to a small extent, 10% not at all). However, despite this sentiment, **when asked for concrete examples of provisions or areas that could be simplified or removed, there were very few responses**. The responses did not always include specific suggestions for simplification measures in the sense of reducing the obligations in the Directives, but rather pointed at broader measures, such as the need to reflect about the optimal way of presenting information, or the need for more guidelines to help simplify the law or using Regulations instead of Directives. Some of the respondents considered that the introduction of new prohibitions to the UCPD blacklist would be a type of simplification measure in the form of more harmonisation of prohibited practices at EU level.

Finally, it should be noted that the analysis regarding the scope for simplification and burden reduction primarily concerns the obligations in the Directives themselves. However, as explained earlier, there are also additional costs stemming from differences in national laws which could be reduced through further harmonisation at EU level.

---

[166] Direction générale de la concurrence, de la consommation et de la répression des fraudes, ' Bilan d'activité 2022', available at: https://www.economie.gouv.fr/files/files/directions_services/dgccrf/dgccrf/rapports_activite/2022/ra-dgccrf-2022.pdf?v=1688637810

[167] Konsumentenverket, 'Årsredovisning 2022', available at: https://stpubshop.blob.core.windows.net/publikationer/arsredovisning-2022-konsumentverket.pdf

[168] The Directives (especially the main provisions of the UCPD and UCTD) are largely principle-based, requiring the traders to act in good faith, refrain from deception and unfair treatment of their customers. There is no room for burden reduction measures regarding these core fairness requirements, as it would imply compromising the core objective of EU consumer protection policy. It is due to this specificity of this legislation that any simplification measures can only be presented as 'limited' in nature.

The main issue highlighted by the data collection and consultations concerns the **volume and nature of information that traders have to provide to consumers**, despite the business survey not identifying the associated costs as significant. Interviews and responses to the public consultation and targeted survey also indicated that the expanding list of information obligations can be burdensome, particularly to SMEs, who are less able to keep up with the changes resulting from different legal instruments, including sector-specific legislation going beyond the three Directives. Information obligations were addressed in the 2017 Fitness Check which only found potential for limited simplification in the area of information obligations as regards information about complaint handling and trader's means of communication. These were subsequently considered by co-legislators in the MD negotiations. The final simplification measures consisted of removing the information requirement about the trader's fax machine number in the CRD and the information requirement about complaint handling in the UCPD.

Concrete suggestions in the consultations of this Fitness Check pointed at the following areas:

- Concerning information obligations about the trader's contact details, in particular the disclosure of the **trader's geographical address**, some stakeholders questioned the need to require the publishing of a geographical address by traders, such as social media influencers, if they are only engaging in marketing practices, but not selling products or services directly to consumers. In the case of influencers, the difficulties with compliance include concerns for the safety and privacy of these traders, who are natural persons who may operate from premises which are also their private residences. At the same time the DSA extends the information requirements allowing for the traceability of traders (Article 30) also to traders promoting messages on products or services on behalf of brands (Recital 72). Thus, online platforms are held to ensure that those influencers can promote product or service on their online interface once they have obtained the required information and disclosed the essential information (such as the geographical address) on its online interface, next to the product/service being offered. A similar requirement for information society service providers to disclose their geographical address in an easy, direct and permanently accessible manner to the recipients of the service has also been enforced by some authorities against influencers under Art. 5 of the e-commerce Directive.[169]
- Regarding digital subscriptions, the **suppliers of audiovisual content streaming services** highlighted the difficulties of ensuring the **14-day right of withdrawal** with respect to their services. Under the CRD, consumers can withdraw from the contract for digital services during 14 days from the conclusion of the contract even after the performance of the contract is started. In contrast, the consumer has no right of withdrawal (subject to the specified conditions) from the contracts for the provision of online digital content after their performance is started. The latter are characterised "by a single act of supply to the consumer of a specific piece or pieces of digital content, such as specific music or video files" (Recital 30 MD). According to the providers in question, if the consumer was to be granted the right of withdrawal from the entertainment subscription and would withdraw during the 14-day period, a *pro-rata temporis* calculation of the compensation due to the provider for the services used before the withdrawal would be inadequate to cover the high cost of the content creation. It would be also complex to calculate such compensation based on the actual costs of the royalty payments disbursed by the provider in relation to the content consumed. These providers explain that, if the right of withdrawal were to apply, a significant share of consumers would consume the most valuable content they are interested in within a

[169] There is a difference in scope between the UCPD and ECD rules, with the latter applying to both B2B and B2C relations and to the provider of services, which is a slightly wider than the notion of "trader" under the UCPD.

short period (over a weekend or in a few days) and would then only incur the compensation obligation of a very small amount if calculated on a *pro-rata temporis* basis from the monthly price of the service.

One streaming service provider in the EU[170] reported that it currently grants refunds as a commercial gesture to users who request cancellation during the first month. These refunds amount to approximately 9 million EUR of ungained revenue per year in the EU (corresponding to the price of a 1-month subscription of the subscribers concerned). 25% of all cancellations of subscriptions to their service in the EU is by users who had subscribed to the service at least twice before, with no more than a year passing since their last subscription. The ratio of such users amongst those who cancel during the first month of their subscription is even higher (40%). According to this provider's projections, if the 14-day right of withdrawal was applied, the total ungained revenues in the EU would amount to about 73 million EUR per year (based on the users' payment for 2 days instead of one full month).

A second streaming service provider in the EU also reported that it grants refunds as a commercial gesture to users who request cancellation during 14 days. In 2023, about 124 000 users benefited from such refunds in the EU, of which 68% were users who had streamed the content for at least 3 days. These refunds amounted to 1 to 1.3 million EUR of ungained revenue (based on the price of a 1-month subscription for the users concerned) and they also generate direct losses due to the royalty payments disbursed by the provider. For comparison, over 1.6 million users cancelled and rejoined this provider's service two or more times in the EU in 2023.

- As regards contracts for online digital content, feedback from interviews highlighted a concern of some traders about having to **inform consumers about their right of withdrawal**, only to have them **immediately waive that right**, which may create a negative perception for the consumer. Therefore, some traders find it better to allow cancellations and refunds at any time. The Commission has clarified this legal matter in the CRD Guidance - in the case of contracts for digital content that are performed immediately and where the consumer provides consent and acknowledgement triggering the start of the performance of the contract, traders do not have to inform consumers about the existence of the right of withdrawal first. Overall, the consultations suggest that certain digital traders experience difficulties with understanding and applying the right of withdrawal, including in terms of distinguishing between digital service and digital content contracts.
- Concerning the purchase of **in-app currencies and virtual items**, e.g. in video games or social media apps, stakeholders asked for more clarity concerning *inter alia* the nature of the contract for the acquisition of virtual currencies and whether their subsequent use to acquire virtual items constitutes a contract. Regarding the latter, the determination of the existence and validity of a contract, which triggers the application of consumer contract law requirements (specifically, information and formal requirements and the right of withdrawal under the CRD), is subject to national law. The CPC authorities discussed these matters in 2024, noting that the treatment of the acquisition of virtual items with in-app currencies under national law (as either separate contracts or as part of the execution of an existing contract) requires a case-by-case analysis. This means that, in some cases, such acquisition is subject to the requirements of the CRD but not in other cases, i.e. the legal status of these transactions is not certain. Concerning the

[170] Commercially sensitive information that the streaming service providers supplied to the Commission for the purposes of this report on anonymized basis.

suggestions for simplification, video game providers considered that a full application of the CRD requirements to the acquisition of virtual items implies providing the consumer with repetitive disclosures and consent requests that may be superfluous, especially if the consumer is fully protected by a 14-day right of withdrawal at the stage of purchasing the in-app currency. Similarly, video game providers considered price information in real currencies to be necessary only when in-app currencies are bought and not at the stage of the subsequent acquisitions of virtual items.

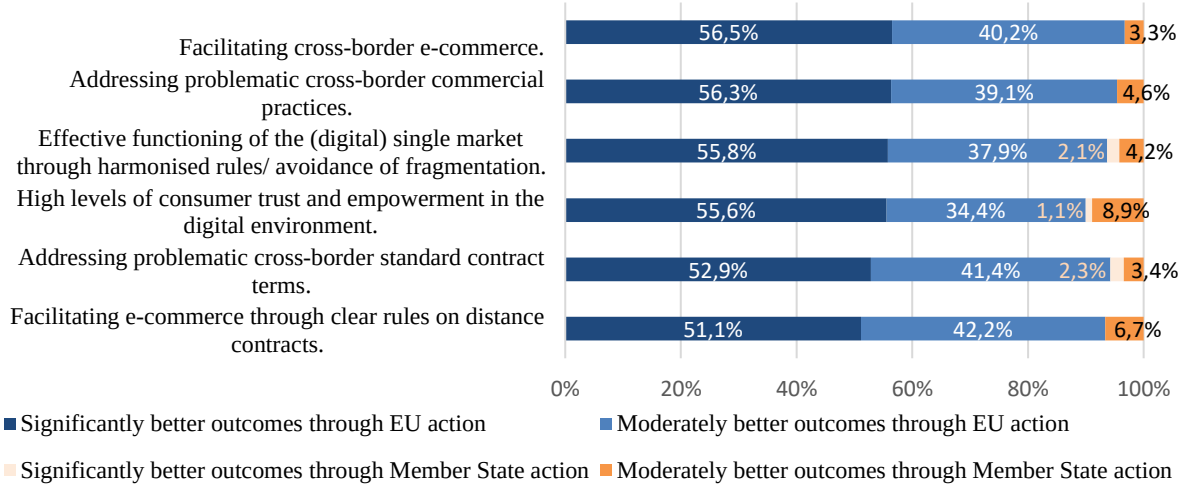
- Concerning contract terms and the associated information overload, there were suggestions to require traders to present consumers with **key T&Cs in a summarised form**, while noting that a large volume of information would nevertheless have to be presented separately for compliance purposes. However, it cannot be qualified as a *per se* simplification measure from the traders' perspective, as they would have compliance costs regarding the development and updating of these summaries.
- Regarding the new rules on **price reductions** in Article 6a of the Price Indication Directive, there were calls for simplification and clarification, including its **interplay with the UCPD as regards other types of price advantages**, which is further assessed in the Commission's implementation report on the MD. In 2021, the Commission adopted guidelines to help with the interpretation of this provision; however, difficulties with its implementation have persisted to a certain degree.

4.2. How did the EU intervention make a difference and to whom?

The main EU added value of the three Directives in the digital environment lies in the establishment of a safety-net of consumer protection with a necessary minimum of regulatory certainty to support the development of digital consumer markets. Furthermore, to the extent that the rules are harmonised across the EU, it enables national enforcement authorities to address cross-border infringements more effectively. Increased EU-level coordination prevents the same infringements from being resolved differently in different Member States.

The targeted survey results show a **consensus about the EU added value of the harmonised rules in the digital area to traders and consumers across the EU**. The majority of respondents consider that the EU consumer law framework has achieved moderately or significantly better outcomes than could have been achieved by Member States in the following areas: facilitating cross-border e-commerce (97%), addressing problematic cross-border commercial practices (96%), ensuring the effective functioning of the digital single market through harmonised rules/avoidance of fragmentation (94%), addressing problematic cross-border standard contract terms (94%), facilitating e-commerce through clear rules on distance contracts (93%) and ensuring high levels of consumer trust and empowerment in the digital environment (90%).

Figure 11 - Stakeholder perceptions of the extent to which the Directives have contributed to the achievement of better outcomes through EU action[171]



Source: Targeted stakeholder survey to support the Fitness Check

The impact of the harmonisation of rules on advertising and standard contract terms for online sales was also explored in the business survey, where **77% of respondents were SMEs**. They recognised a positive impact on trust among consumers concerning making purchases of goods, services or digital content online (87%), ensuring fairness for consumers in the digital environment (80%), striking the right balance between consumer protection, whilst not overburdening traders (79%), creating a level playing field across the EU for businesses regarding advertising (79%) and improved regulatory certainty for businesses (77%). The impact of harmonisation on facilitating cross-border trade was also recognised, but to a lesser degree (60%), which points to the importance of additional factors that may hinder traders from selling cross-border, such as language barriers, delivery costs, logistics etc.

The effective functioning of the digital single market cannot be achieved through national laws alone. The EU added value is particularly evident in the CPC cross-border enforcement cooperation actions and related activities, which would not be possible without a common legal framework. Both maximum and minimum harmonisation rules in the three Directives have helped to reduce obstacles and cut costs for traders. The UCPD in particular has replaced diverging regulations across the EU by providing for a uniform legal framework, including through the introduction of an EU-wide blacklist of prohibited commercial practices.

Several stakeholders and Member State **respondents called for more harmonisation in the future**, including the expansion of the UCPD blacklist and the introduction of an EU-wide UCTD blacklist of unfair contract terms, while leaving Member States the possibility to prohibit additional unfair terms. Furthermore, the analysis of problematic practices in Annex VI points at several aspects that are formally within the material scope of the Directives but not sufficiently harmonised, which has contributed to increasing the risk of regulatory fragmentation with Member States adopting different national approaches (e.g. on cancellation and renewal of digital subscriptions or influencer marketing).

[171] "To what extent has the EU consumer law framework achieved better outcomes than could have been achieved by Member States regulating these areas themselves?" (n=95)

4.3. Is the intervention still relevant?

The consultations and data collection confirm that the **objectives of the three Directives remain highly relevant in the digital environment**: the EU must ensure a high level of consumer protection and a better functioning of the internal market through harmonised rules. Until now, the Directives have provided a necessary baseline of consumer protection and contributed to the better functioning of the Digital Single Market. However, the digital environment presents specific challenges that are not present in the offline environment in the same form or scale. Behavioural research has shown that consumers do not behave exactly the same way online as they do offline, and traders have unprecedented means to increase the effectiveness of online commercial persuasion. The Fitness Check shows that there is a continuation of the same problems of power imbalance between consumers and traders that triggered the EU intervention and subsequent amendments in the past, now amplified by the increased scale, speed and potency of digital solutions for targeting consumers. In their current form, the three Directives are only partly reflecting the current and future consumer protection needs. As explained in the section on 'effectiveness' - technological and market developments have made the average consumer more vulnerable and increasingly dependent on data-driven services, and they find it difficult to make informed choices in dynamic online choice architectures.

Current and emerging needs

According to a Eurobarometer survey from June 2023 for the Digital Decade policy programme, 79% of EU consumers consider that digital technologies will be important in their lives by 2030. However, only 50% consider that digital rights are currently well protected in Europe and less than half think that the digital environment is safe for children and young people. When facing these challenges, consumers that lack digital skills are likely to be more susceptible to unfair digital practices. The EU has committed by 2030 to ensuring that 80% of those aged 16-74 obtain basic digital skills, but the first report on the Digital Decade from 2023 estimates that under current conditions, only 59% will achieve this. These developments highlight the **importance of maintaining a strong consumer protection framework that does not only focus on providing consumers more information but that ensures consumer protection by design and by default.**

The Commission's 2023 foresight study, which examined the impacts of the twin transitions and the COVID-19 pandemic on consumer behaviour, consumption patterns and markets in Europe with a time horizon of 2025 to 2030, highlighted the importance of data privacy and personalisation for consumer policy. The study concluded that EU consumer protection must focus even more on online shopping and other online activities in the future in order to identify and reduce the risks relating to people's vulnerability, especially in terms of physical and mental health, income and social participation, as well as privacy, data protection and freedom of choice in consumption. Personalisation can increasingly define not only what consumers see or want to buy, but also whether they even have access to the product or service (e.g. get a loan or insurance), which can have a strong influence on consumer behaviour and become a social challenge. Concerns have also been raised about **digital dependence and the widening of the digital divide between consumers that have access to digital technologies and those not willing or capable of using them**. Vulnerable consumers might no longer have full access to products and services on the market, and all consumers may face increasing difficulties in having access to a human interlocutor, especially with the increased use of AI chatbots. Several stakeholders call for the introduction of a new consumer right to access a human interlocutor in the customer service context.

Several stakeholders, including national authorities, consider that the specific vulnerabilities of **children** are still not sufficiently recognised, in line with the UN General comment No. 25 on children's rights in relation to the digital environment. The Directives do not contain specific protections, aside from the reference in the UCPD to children as a group of vulnerable consumers from whose perspective unfair practices could be assessed and a prohibition of direct exhortations to children to buy products.

The Directives also do not have any specific requirements for traders concerning accessibility for **persons with disabilities** or other relevant protections, in line with the UN Convention on the Rights of Persons with Disabilities. However, specific requirements have been introduced at EU level through the European Accessibility Act and the Web Accessibility Directive as regards the accessibility of the websites and mobile applications of public sector bodies and on the accessibility requirements for products and services (including B2C e-commerce services), with the latter becoming applicable from 28 June 2025. Moreover, both the DSA and AI Act foresee the adoption of codes of conduct that should also take into account accessibility aspects for persons with disabilities. Furthermore, the proposed horizontal Equal Treatment Directive would prohibit discrimination on several grounds including disability *inter alia* in the area of access to goods and services.[172]

The Directives are also **limited in terms of their ability to capture all types of consumer harm that can occur in the digital environment**. For example, the 2023 EP resolution on addictive design outlines a multitude of psychological, physical, societal and economic harms that are associated with digital addiction, which include depression, social pressure and obsessive-compulsive symptoms, including compulsive buying. In their current form, the three Directives do not specifically address physical or mental health concerns. The UCTD does not refer to health, whereas Article 3(3) UCPD specifically provides that the Directive is without prejudice to EU or national rules relating to the health and safety aspects of products, and the CRD excludes healthcare contracts from its scope. Furthermore, legal uncertainty about concepts such as the consumer's 'transactional decision' in the UCPD, undermines its application in a digital environment that is increasingly focused on capturing the consumer's attention and increasing engagement, not only getting consumers to make purchases. Overall, the **Directives cannot be considered as having made a significant difference outside of the immediate sphere of protecting the economic interests of consumers in direct purchasing decisions** in the digital environment. In contrast, in the area of consumer safety, the objective of the recently adopted General Product Safety Regulation (GPSR) is to protect the health and safety of EU consumers. The GPSR strongly underlined that **'health' is to be seen as a state of complete physical, mental and social well-being, and not merely the absence of disease or infirmity**. Accordingly, it requires that mental health risks are also taken into account when assessing the safety of products. The inclusion of similar values could be considered more horizontally in EU consumer law to further enhance the protection of consumers in the digital environment.

Online practices harmful to the environment, such as those fostering overconsumption or impeding sustainable consumption, can impact consumer welfare. In order to contribute to the proper functioning of the internal market, based on a high level of consumer protection and environmental protection, and to make progress in the green transition, it is essential that consumers can make informed purchasing decisions and thus contribute to more sustainable consumption patterns also in their online transactions. This would contribute in particular

[172] Text retrievable at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52008PC0426. The most recent Progress Report has been submitted to the EPSCO Council on 14 June 2024.

towards the **UN Sustainable Development Goals no. 12 (ensure sustainable consumption and production patterns) and no. 13 (climate action).** Traders should provide clear, relevant and reliable information, and they should not engage in unfair, misleading or aggressive practices that foster overconsumption or impede sustainable consumption. For example, consumers can be hindered from making more sustainable choices by dark patterns, addictive design and aggressive or unsolicited personalised advertising that are aimed at getting them to buy more goods and services. Similar problems occur when digital subscriptions are difficult to cancel or when they automatically renew themselves, without the consumer's express consent or despite the consumer not using them. If the Directives are correctly applied and broadly interpreted, then they can be used to limit the effects of such problematic practices. However, the **Directives are currently not specifically addressing the links between the digital environment and the green transition**.

Technological developments

There are several technological developments that will impact the relevance and fitness for purpose of the three Directives in the future. This can involve the **emergence of new technologies or the increased take-up of technologies that have existed for some time**.

The growing use of **artificial intelligence**, with its complexity and opaqueness, is expected to exacerbate the imbalances between traders and the average consumer, who lacks comprehension and awareness about how these tools are developed, what inputs they use and how a particular output is determined. Generative AI models reproduce existing materials and may generate misleading information, inaccuracies, hidden advertising and exploit consumer vulnerabilities. Potential consumer over-reliance on the outputs of such models or on automated contracting can also lead to reduced consumer agency, for which digital skills are essential. Furthermore, some stakeholders have raised **concerns about emotion-recognition AI and anthropomorphic AI systems that emulate human communication and emotions**. The use of such systems in commercial practices could distort consumers' decision-making, even if it is clear to them that they are interacting with an AI system. Most consumers believe that AI can bring benefits, but there is a need to raise awareness of the risks and educate consumers about when and how AI is used. A representative EU consumer survey showed that over half of consumers thought that companies are using AI to manipulate their decisions and less than 20% felt that current rules can adequately protect them from potential harms.[173] The AI Act addresses several issues through prohibitions and new requirements in particular for 'high-risk' AI systems and general purpose AI, but most consumer-facing AI systems are 'low risk' and are not expressly regulated. Multifaceted concerns remain regarding the use of AI in commercial practices ranging from personalised advertising to the use of AI chatbots in customer service. It should be seen whether some of these concerns can be addressed through the Commission's implementing guidelines on the prohibitions and codes of conduct envisaged in the AI Act to which providers and deployers can voluntarily adhere to.

The rapid proliferation of **connected devices**, driven by cloud-based infrastructure and services, edge computing capabilities and telecommunications network developments will change how consumers interact with traders and raise questions, among others, on how pre-contractual information will be communicated to consumers. The emergence of **smart contracts and automated contracting**, including autonomous AI-powered contracting, could increasingly automate all stages of the consumer's transactional journey, including the full life cycle of a contract from conclusion to execution. Challenges related to automated contracting are further

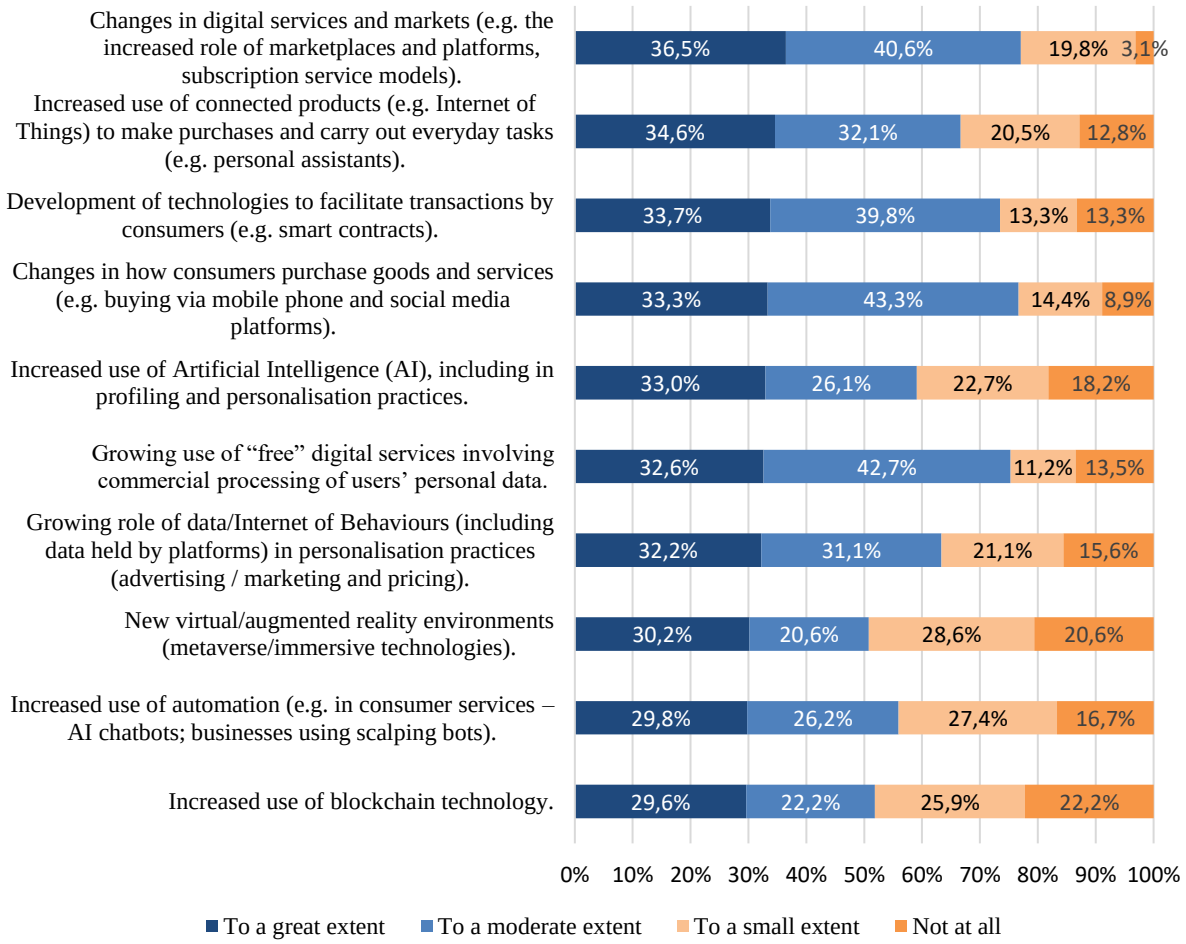
[173] A representative survey commissioned by BEUC, covering 1000 consumers per country in BE, IT, ES, PT and 1500 consumers per country in DK, FR, DE, PL, SE.

considered in Annex VI. Advancements in **virtual or augmented reality** environments will literally introduce a new dimension to trader and consumer relations. The Commission's 2023 Communication on virtual worlds noted that EU consumer laws, in particular the UCPD, would fully apply to B2C practices in such environments. The EP's 2024 resolution on virtual worlds acknowledged that there could be significant risks in the area of consumer protection, including the exacerbation of the imbalances between traders and consumers, and encouraged the Commission to conduct regular checks of the adequacy and consistency of the legal framework in the future, as these technologies become more mainstream.

In terms of stakeholder perceptions, 60% of consumers responding to the representative consumer survey considered that consumer rights have not sufficiently kept up with technological developments. Nevertheless, most respondents had a balanced view of the situation, stating that 'some uncertainties remain' (44%), rather than 'consumer rights are not sufficiently tailored to meet digital challenges' (16%). Based on additional data provided in the survey, consumers who had a more positive attitude towards spending time online and those with lower educational levels were more likely to be optimistic about the status quo of the legislative framework.

Many stakeholders responding to the targeted survey considered that the Directives had addressed digital market trends to a great (35%) or to a moderate (36%) extent, for example as regards the increased role of online marketplaces and platforms. The Directives were perceived to be less adapted to the increased use of AI (including in profiling and personalisation practices), blockchain technology, automation (e.g. AI chatbots, scalper bots) and new virtual/augmented reality environments, with 40-49% considering them not up to date at all or only to a small extent.

Figure 12 - Stakeholder perceptions of the Directives' fitness for market developments and new technologies[174]



Source: Targeted stakeholder survey to support the Fitness Check

Across different consultations, the changes introduced to the Directives by the MD were perceived by stakeholders as having made a positive difference in strengthening their fitness for purpose and relevance in the digital area (responses to the targeted survey: 49% some positive difference, 15% significant positive difference).

Responses to the business survey showed that traders across different Member States are relatively optimistic about the current state of EU consumer law's adaptation to new technological developments – overall, 16% of traders thought that current consumer legislation was very well adapted and a further 76% considered it to be well adapted to new technological developments.[175] Companies of 50-250 employees were the most negative with 21% indicating legislation was poorly adapted.

A recurring element in the position papers and interview responses from traders and business organisations was that the existing rules should be enforced to their fullest extent before proposing any legislative changes. Industry representatives are concerned that, taking into account the new and recently updated legislative acts regulating different aspects of digital products, services and technologies, additional legislative changes could lead to confusion,

[174] "To what extent do the three EU consumer law Directives keep up with the following specific evolving developments in digital markets and new technologies?" (n=96)

[175] Spanish traders were the most positive with 100% indicating legislation was well or very well adapted, while Portuguese traders provided the most negative responses with 22% of companies indicating legislation is poorly adapted.

uncertainty and further legislative fragmentation, as well as create a bias against digital trade channels to the detriment of consumer choice and the competitiveness of EU businesses globally.

Safety-net framework

Aside from the differences in perceptions regarding the impact that new technologies will have on the relevance of the three Directives, all stakeholders recognised the **value of maintaining a technology-neutral and channel-neutral approach to ensure that the safety-net remains future-proof**. There was a consensus about the importance of preserving this general framework, as a complement to more specific rules. The UCPD and UCTD in particular can provide a broad safety-net of protection in various areas not explicitly addressed by new digital legislation, as acknowledged for example in Regulation (EU) 2023/114 on markets in crypto-assets, when referring to offers of crypto-assets other than asset-referenced tokens or e-money tokens (Recital 29).

However, despite the advancements brought by the three Directives during the evaluation period, their practical relevance is likely to diminish in the future in view of the challenges with the effectiveness described earlier and the entry into application of several new EU legislative instruments in the digital area, such as the DSA, DMA and AI Act. Several of these laws can be viewed as having 'fully regulated' specific problems, sectors or technologies. Without the further development of consumer rights and without reinforcing enforcement (ensuring resources and facilitating coordination, cooperation, capability building and swift mutual assistance) in the future, there is a risk that horizontal EU consumer law would lose relevance, as it will only be used if action has not already been taken by other authorities on the basis of other areas of EU law. This could be the case even if the complementary application of consumer law is not legally precluded.[176] Nevertheless, the Directives continue to ensure certain remedies for harmed consumers that are not present in other legislation, and which could be used in private enforcement actions.

In practice, it is likely to become increasingly difficult to ensure an effective and coherent application of EU consumer law regarding the same traders and their commercial practices that fall under the scope of different legislation. The enforcement focus may increasingly shift to data protection, competition law, platform regulation and other areas, as well as towards governance decisions being increasingly delegated to standardisation bodies or to the traders themselves. Furthermore, these activities will be accompanied by additional guidelines and case law that interpret the numerous legal concepts that interface with provisions in the three Directives. Over time, these developments could create the **risk of diminishing the importance of the consumer policy perspective and deprive courts and consumer protection authorities from developing the necessary expertise to assess the commercial practices in digital markets**. The Commission's 2023 foresight study recommended to anticipate possible future gaps in consumer protection legislation and to take action to adjust legislation where necessary and possible, especially for new business models and forms of consumption in the digital world, with a view to introducing more sustainable models.

5. What are the conclusions and lessons learned?

The conclusions of the Fitness Check should be read in the context of the limitations and uncertainties of the evidence base, taking into account the analytical challenges related to the

[176] For example, given the broad scope of the UCPD, it can be applied to most B2C commercial practices even if there is sector-specific legislation in place. The latter would only prevail over the UCPD in case of conflict between the provisions of the UCPD and other EU law regulating specific aspects of those unfair commercial practices.

fast-evolving nature of digital markets and new technologies. Data and stakeholder feedback gathered for the purpose of this Fitness Check clearly point to a strong link between the application of the Directives and consumer protection in the digital environment. However, there are challenges associated with isolating and attributing various effects directly to the Directives and with disentangling the online and offline impacts. The Fitness Check entails a mixed method approach, gathering complementary sources of information over the course of 2 years, including observational market data, behavioural insights, case studies and quantitative data on key effects (consumer detriment and business costs). The analysis also relies on opinion-based survey data, which is needed because of objective limitations related to the subject matter and given the absence of any monitoring and reporting obligations for traders and Member States in the Directives. Despite the above, the main conclusions reflect the commonalities identified and are consistent with previous evaluations in this area.

Conclusions

As a result of the development of EU consumer law over the last 50 years, EU consumers are among the most protected in the world, online and offline. The Fitness Check confirms that the technology-neutral nature of horizontal EU consumer law, with its combination of principle-based rules and more prescriptive obligations and prohibitions, is a necessary component of the regulatory framework for the Digital Single Market. The core objectives of the Directives remain just as valid today. The Directives have provided the **necessary minimum of regulatory certainty and consumer trust to support the development of a diverse market of consumer-facing digital products and services in the EU**.

At the same time, the Fitness Check shows that the Directives have **only partially achieved the objectives** of providing a high level of consumer protection and a better functioning of the internal market through the harmonisation of rules in the digital environment. The Fitness Check indicates the increasing prevalence of multifaceted problems that consumers encounter in the digital environment, including deceptive or addictive interface designs and functionalities, personalised practices targeting vulnerabilities, difficulties with the cancellation and renewal of digital subscriptions, forced acceptance of unfair contract terms and challenges associated with social media commerce. A conservative estimate quantifies the post-redress **financial consumer detriment resulting from problems experienced in the digital environment at EUR 7.9 billion per year, with the highest levels of detriment among younger age groups.** Meanwhile, to the extent that the costs can be quantified and attributed, the regulatory burden for businesses is modest and the Directives do not contain any reporting obligations. The overall estimated adjustment and administrative costs associated with compliance with the Directives across the EU27 amount to approximately EUR 511-737.3 million per year. These estimations illustrate the general magnitude of costs, however, most traders find it difficult to meaningfully distinguish between the costs they face in the online or offline context, as well as between obligations stemming from EU legislation or national laws. Overall, only 10-18% of traders report high costs relating to the different compliance activities, whereas the majority face low costs or no costs at all. The Fitness Check identified some limited potential for simplification and burden reduction, specifically in the area of information requirements and the right of withdrawal, which could be further analysed.

Consumers do not behave the same way online as they do offline. In the online context, they are less likely to pay attention, to read contract terms carefully or to process all of the information they are shown at each step of their transactional decisions. Traders are able to use more effective online commercial persuasion tactics than ever before. Technological developments and insights from the tracking of consumer behaviour are making consumer-

facing digital products, services and business models increasingly complex, for both market participants and authorities. This Fitness Check indicates a **continuation of the same problems of power imbalance between consumers and traders that triggered EU action in the past, now amplified by the increased scale, speed and potency of digital solutions for targeting consumers**. Furthermore, it is clear that several problematic practices identified in the Fitness Check (such as dark patterns) cannot be adequately solved by merely equipping consumers with more information. The Fitness Check outlines the broad categories of issues identified, the evolution of their scale and magnitude over the evaluation period, and examples of possible solutions that emerged during the consultations and data collection. However, the Fitness Check specifically **refrains from prejudging any future prioritisation of issues and the content or format of the follow-up action**. This is the role of impact assessments if further regulatory intervention is deemed necessary in the future.

The Fitness Check underlines the fact that the effectiveness of the three Directives is diminished by **insufficient legal certainty about the application of the existing general principle-based rules to complex online practices**. Despite the benefits of a principle-based approach, the broadly worded legal provisions in the Directives are not specific enough to allow them to be applied effectively to commercial practices and system architectures in the digital environment. Traders are unable to translate these general principles into concrete development decisions on design interfaces, software, hardware, infrastructure etc. Nor do general principles aid the use of automated enforcement tools, which are becoming increasingly necessary in order to track infringements in fast-developing digital markets.

The role played by EU consumer law as a 'safety-net' continues to be recognised and valued. However, the rapid changes in the regulatory landscape since the last Fitness Check in 2017 have increased the **complexity of applying consumer protection rules in the digital area in conjunction with other digital legislation** that provide rules concerning certain types of traders (e.g. online platforms) or technologies (e.g. AI systems). There is also a risk of **regulatory fragmentation** in specific areas in the absence of EU-level action due to diverging national laws and interpretations. Several Member States have adopted or are considering adopting new consumer protection laws in specific areas, such as influencer marketing and digital subscriptions. At present, the level of consumer protection may vary depending on the Member State in which consumers reside, the trader's location, business model or the categories of personal data or underlying technologies that are used in their products or services.

The Fitness Check importantly indicates that **enforcement remains insufficient** despite the new possibilities of collective redress and the continued improvement of the cross-border coordination of public enforcement within the CPC network. The CPC network could deal with cross-border infringements affecting consumers in several EU/EEA countries, thus increasing the efficiency and consistency of EU consumer law enforcement. Without the CPC system, consumer protection authorities would need to engage in numerous parallel proceedings at national level against the same trader, leading to higher costs and different levels of consumer protection across the EU and thus an uneven playing field. However, as outlined in the 2024 application report on the CPC Regulation, several challenges continue to undermine the ability of the CPC network to be fully effective in digital markets. These include limited resources, the length and complexity of procedures, the need for specialised expertise and the absence of tools to detect infringements. The Commission is currently reflecting on the **possible need to reform the CPC Regulation in order to strengthen it.**

In practice, all three Directives lack sufficient national and CJEU case law applying them in the digital environment, especially to new technologies and data-driven practices. This leaves **EU**

consumer law largely underused when it comes to meeting its intended objectives. Authorities, consumer organisations and other plaintiffs would have to take considerable risks and face a difficult burden of proof in order to test the application of these laws. Similarly, **law-abiding traders do not have sufficient certainty that the measures they are taking are enough to ensure compliance,** and they lack incentives to go the extra mile in a competitive environment that does not reward 'digital fairness by design'. While the Commission's interpretative guidelines are perceived very positively by authorities and market participants alike, they are not binding and cannot create sufficient incentives to ensure effective implementation. Voluntary initiatives, such as codes of conduct or pledges, can likewise improve implementation of EU consumer law and facilitate policy dialogue but ultimately cannot overcome shortcomings in the legislative framework.

Lessons learned

To achieve digital fairness, the Fitness Check points to the need to do more to address the remaining consumer protection challenges in the digital environment. A key lesson learned is that **a strong and self-standing consumer protection framework brings added value when assessing evolving commercial practices in digital markets**. The existing EU legal framework cannot be considered sufficiently effective in tackling current and emerging consumer harms. In the absence of further action, EU consumer law will not fully meet its objectives, risks losing relevance in the digital area and may continue being applied only in limited cases.

At the same time, the Fitness Check acknowledges the **limitations of this evaluation**, considering that more time may be needed for the implementation of recent EU digital legislation in order to appraise its effects on consumer protection. While it is **difficult to predict the extent to which the new digital rulebook can compensate for the absence of concrete and well-defined digital consumer rights in EU consumer law**, it is clear from the material and personal scope of the new laws that the scale of the challenges that are meant to be regulated by EU consumer law and other laws remains significant[177]. There is a need for **continued monitoring and periodic evaluations in this area,** and further regulatory updates in the future cannot be precluded. Stakeholder discussions should continue about the future of digital consumer protection, including about the specific role of EU consumer law and its enforcement in the 'new digital order' of EU legislation. In this context, the Fitness Check presents areas for further analysis, rather than specific recommendations.

This Fitness Check strives to establish a baseline that can be used for monitoring developments and further built upon in the future for any new policy initiatives. To alleviate the limitations and uncertainties related to the evidence base and to provide a better baseline, specific measures could be explored in the future to **improve the monitoring and evidence-collection processes** in this area. Currently, the Directives do not include any monitoring or reporting requirements, which creates difficulties for evaluation purposes. Certain data gaps relate to information that could best be gathered at national level, such as the estimates regarding the costs for traders and the resources and capacities of national authorities. It could be beneficial to obtain a systematic overview of court cases, enforcement actions and other enforcement activities at national level, with sufficient granularity in the data to distinguish between the type of legal instrument involved, the subject matter and whether it pertains to online or offline matters. In general, the

[177] As explained in section 4.1.2.2, the new Acts did not intend to cover all problematic practices, digital services or types of traders relevant in B2C markets.

collection of quantitative data could be significantly improved, including quantitative estimates of effects on a general macroeconomic level related to consumer policy.

To improve the use of consumer and economic data for policy making, the use of various statistical tools could be further explored in addition to the systematic and standardised mapping of the digital markets (e.g. regular reports on key data) with the aim of obtaining objective and meaningful data. Similarly, the evidence base could be strengthened through a better structured reporting on consumer complaints. Other means of improving the collection of data directly from consumers regarding digital matters could also be used, in particular maximising and further refining the use of existing tools such as the ECC Network or special Eurobarometer surveys. More emphasis could be placed on developing **automated market sweep tools**, **which would reduce the reliance on complaints data and qualitative opinion-based data**. Automated tools could also help safeguard the relatively low administrative burden of EU consumer policy whilst increasing its level of effectiveness. Such tools could benefit both monitoring and enforcement. For example, the EU eLab is a digital toolbox developed by the Commission to support national authorities with their online investigations. It contains several digital enforcement tools, including AI-based tools that can be used to detect infringements taking place in digital markets.

As in the past, data gaps concerning specific problems could also be filled through studies commissioned on an *ad hoc* basis, depending on the needs identified. For example, building on the data gaps identified in this Fitness Check, the Commission has launched additional studies to gather more evidence and support the capacity of national enforcement authorities. These studies concern online marketing techniques used in video games that adversely affect the purchasing behaviour of children, transparency of price promotions on e-commerce websites, use of AI chatbots in customer service, and labelling of commercial content in social media.

Without prejudice to the format and content of future Commission action, the lessons learned from this Fitness Check point to the following **areas for improvement** regarding the Directives, which could be further analysed:

1. **addressing the most harmful problematic practices** so as to increase consumer trust in digital technologies, reduce consumer detriment and enable consumers to make more meaningful and informed choices in the digital environment;
2. **reducing legal uncertainty** for market participants about the application of EU consumer law to practices in the digital environment, **preventing regulatory fragmentation** between Member States and **promoting fair growth and competitiveness** in the digital economy;
3. **ensuring the consistent application** of EU consumer law and other EU legislation that regulates aspects of B2C digital markets, new technologies and the use of consumer data for commercial purposes;
4. **facilitating more effective enforcement and compliance with** EU consumer law, in particular in technologically complex cases, and reflecting on how to address current challenges for the cross-border enforcement of consumer protection;
5. **simplifying the existing rules in the areas identified**, without compromising the objective of a high level of consumer protection.

Furthermore, in the area of coherence, the following areas could be further explored to ensure a **stronger, more consistent and coherent application of the broader EU digital rulebook** affecting consumers, such as:

- providing greater legal certainty about the scope and content of the laws and their interplay with consumer law, e.g. by adopting or updating Commission guidelines;
- facilitating closer cooperation between different enforcement authorities and their respective networks, e.g. following the example of the DMA High Level Group, which formally brings together different authorities (including competition and consumer authorities) or more informally, such as the 'group of volunteers' of data protection authorities and CPC network's consumer protection authorities that meet to establish best practices and share enforcement experiences; furthermore, in 2023, the European Data Protection Board established a taskforce on the interplay between data protection, competition and consumer protection law;
- providing a legally sound framework for cooperation and the exchange of information between competent authorities, while preserving due process and procedural rights for businesses under investigation;
- further engaging with traders both at national and EU level in 'preventive' or 'positive' enforcement in order to facilitate compliance with the broader legal framework, e.g. preventive cooperation, negotiations and dialogue to address the concerns of consumers and enforcement authorities;
- funding projects that seek to improve awareness of and train businesses across the EU on the applicable digital laws, e.g. following the example of the Consumer Law Ready project that trains SMEs on EU consumer law;
- developing market monitoring and IT tools that may be relevant for multiple digital laws in order to facilitate compliance and enforcement, e.g. digital observatories, automated tools, and EU-level databases of problematic practices.

Annex I: Procedural Information

Lead DG/Decide reference/Work Programme

Lead DG: DG JUST

Decide Planning: PLAN/2022/561

CWP references: CWP 2024, Annex II, Section C, point 2

Organisation and timing

The Fitness Check initiative was published in the Have Your Say portal in March 2022, followed by the publication of the Call for Evidence in May 2022, setting out the context, scope and aim of the exercise for the public. A public consultation took place from 28 November 2022 to 20 February 2023. Additional surveys and data collection activities were carried out by an external contractor in 2023.

An Inter-Service Steering Group (ISSG) was set up in March 2022. In addition to the Legal Service (SJ) and Secretariat General (SG), 11 Directorates-General assisted DG JUST in the preparation of the Fitness Check report: DG for Financial Stability, Financial Services and Capital Markets Union (FISMA), DG Internal Market, Industry, Entrepreneurship and SME (GROW), DG Communications Networks, Content and Technology (CNECT), DG Mobility and Transport (MOVE), DG for Trade (TRADE), DG for Health and Food Safety (SANTE), DG Environment (ENV), DG for Employment, Social Affairs and Inclusion (EMPL), DG Competition (COMP), DG Energy (ENER) and Joint Research Centre (JRC). In addition to targeted consultations in writing, the ISSG held meetings on 22 April 2022, 7 November 2023 and 14 March 2024. Pursuant to the requirements of the better regulation guidelines, the minutes of the last meeting were submitted to the RSB.

Consultation of the Regulatory Scrutiny Board

The RSB was consulted in an upstream meeting on 19 June 2023. The draft Fitness Check report and all supporting documents were submitted to the RSB on 25 March 2024 and a hearing was held on 24 April 2024. After the hearing, the RSB issued a negative opinion on 26 April 2024. The RSB's general comments were the following:

(1) The report is not sufficiently clear about the robustness of the evidence base. Its methodological approach has significant shortcomings in terms of points of comparison and attribution.

(2) The report is not clear on the existence and size of the gap between existing consumer legislation and the digital acquis nor on the scale and development of problems identified. The report does not sufficiently identify and analyse enforcement deficits and does not address the role that Member States national rules and their administrative capacities play.

(3) The impacts of consumer law on businesses and SMEs are not sufficiently clear. Cost estimates and the simplification potential are not sufficiently addressed.

The specific comments elaborate on these aspects. The following table explains the key issues raised by the Board and the adaptations introduced to the report.

RSB comments – What to improve	Adaptations introduced
(1) The description of the evidence base requires significant improvement so that it is clear how robust and representative the evidence is. In this respect, the report should clarify what data is statistically representative and how it was analytically quality assured. The representativeness of the pre-established large-scale panel used for the consumer survey should be better explained. The report should critically assess the limitations and uncertainties of the evidence and the sources of the data, in particular perception based, and how this may affect the quantitative results. Any quantitative analysis and reporting of non-representative data based on small samples should be done with utmost caution and only where appropriate. It should include and compare the perception based data with other types of data, such as complaints data on revealed preferences in actual transactions.	Additional explanations on all of the primary evidence sources were added in Annex II, including information on their robustness, representativeness of survey, purpose, complementarity and use. Overall, the evidence base entails a mixed method approach, gathering complimentary sources of information over the course of two years, including observational market data, behavioural insights, case studies, quantitative data on key effects extrapolated to the EU27 (consumer detriment and business costs) and representative survey data (consumer and business surveys). A delineation of the main methodological and evidence-related limitations was provided in Annex II and up-front in section 2.2 on points of comparison. The limitations were highlighted once again in section 5 on conclusions and lessons learned, along with a proposal to improve the monitoring and evidence-collection processes in this area.
(2) The report should clearly identify, with concrete evidence where already available, the scale of the remaining gap between the consumer legislation covered by the report and the evolving digital acquis. Where there are gaps in evidence due to the evolving situation, this should be explicitly mentioned, along with the need to undertake further analysis in view of potential new initiatives. It should explain to what extent new obligations imposed under the Digital Markets, Digital Services and other recent Acts may tackle part of the emerging problematic digital practices faced by consumers, for instance via obligations imposed on major gatekeeper platforms. In relevant situations, the report should clearly delineate and analyse the scale of the "residual" problem, e.g., the	The remaining challenges for consumer protection following the adoption of recent digital legislation were more clearly highlighted with a new sub-section in 4.1.2.3 on external coherence. It was explained that the scale of the residual challenges that were meant to be regulated by EU consumer law and other laws remains significant, while the potential benefits of the new digital legislation on consumer protection were clearly recognised. In addition to identifying the gaps, it was explained that there is scope for the parallel application of EU consumer law, which brings regulatory complexity, legal uncertainty and potential incoherence. The potential measures that could be taken in the interim to ensure a strong, consistent and coherent application were presented in section 5 on conclusions and lessons learned.

scale of the problem outside of the major gatekeeper platforms.	
(3) The report should significantly improve the analysis so that it is clear what has happened in the evaluation period (2017-2023). It should identify appropriate points of comparison and explicitly reference how much change has happened relative to those points. It should be clear how much change can be attributed directly to the three Directives in scope and to what extent this change meets the original expectations.	New analysis was developed, significantly expanding section 3 on how the situation has evolved over the evaluation period, covering key data on B2C digital markets, consumer awareness of their rights, consumer complaints (put into the context of digital growth), evolution of specific problems, a retrospective quantification of consumer detriment since 2017, overview of other harms beyond financial detriment and key points regarding implementation and application. The changes relative to the baseline are clearly explained (to the extent that there is available comparable baseline data for each problem and with caveats about the limitations of attributing changes directly to the three Directives). Moreover, section 2.2 on points of comparison was revamped, highlighting all of the relevant indicators of success. For the purposes of direct comparisons, data points were provided for the monitoring indicators in the 2018 Impact Assessment accompanying the MD, showing that there has not been sufficient progress towards achieving the targets that the Commission established.
(4) The estimates of the consumer detriment should be better explained and evidenced including the key assumptions (in particular the assumption of the 30% of EU consumers experienced problematic practices in 2023). The estimated consumer detriment should not be regarded as a cost to consumers due to the legislation, but the analysis should show whether it has increased or decreased (and by how much) in the evaluation period relative to the point of comparison.	Extensive new analysis was developed on consumer detriment in section 3, examining sequentially: consumer participation in digital markets, consumer awareness of their rights, number of consumer complaints, scale of specific problems, quantification of revealed post-redress financial detriment and an overview of other harms, including mental harm. It was clearly explained that the underlying assumption that approximately one third of consumers (30%) face problems online is based on figures from two representative surveys from the Commission, which together account for over 37 000 EU consumer experiences. Consumer detriment was no longer presented as an 'indirect cost' from the Directives, but instead characterised as a result of non-compliance with the Directives or as a kind of unrealised benefit that was intended to result from the correct application of the Directives.
(5) The report should be more explicit on the relative scale and the relative	Extensive new analysis was provided in section 3 on the relative scale and importance of the

importance of the problems. It should place the estimates of the consumer detriment and the number of consumer complaints in the right context. In doing so, it should assess the scale of the problem relative to the overall consumer spending in the digital economy so that the magnitude of problematic consumer transactions becomes more apparent. It should demonstrate how the problem has evolved over time, for instance, by comparing the growth rate of the e-commerce / services sectors with the share of consumer complaints.	problems. Consumer complaints were put into context and interpreted more meaningfully by neutralising the effect of digital market growth, e-commerce uptake and inflation. New figures were added in the descriptions of the specific problematic practices using representative survey data (e.g. CCS, consumer survey, Eurostat) and secondary sources from desk research, which was contrasted by the change in market size and structure during the evaluation period.
(6) The report needs to better address the issues of unavailability of robust evidence based on quantitative non-opinion data. Regarding emerging problems, the report should better analyse the severity/harm, e.g. related to mental health and other aspects of consumer detriment beyond direct financial losses. In case relevant data or evidence is not available the report should clearly outline the evidence gaps and could propose steps towards collecting the needed evidence.	In addition to the adaptations described under comment 5, new analysis was developed in section 3 sub-section 'other harms'. Supported by additional scientific data and desk research, it was explained that the problematic practices identified in the Fitness Check can lead to multifaceted consumer harms beyond financial detriment that directly or indirectly impact the consumers' economic interests and the collective interests of consumers. The evidence base regarding the scale and severity of the risks that consumers face has been increasing over the evaluation period; however, scientific research is still evolving on certain emerging issues, especially given their relative novelty (e.g. addictive design, AI chatbots) or limited spread in mainstream consumer markets (e.g. virtual worlds). Steps towards the improvement of monitoring and data collection were proposed in section 5 on conclusions and lessons learned.
(7) The report should analyse and take into account differences between Member States. It should explain whether the consumer survey results, and other stakeholder feedback showed any significant differences regarding the relative scale of the explored problematic practice and if so, explain the reasons behind (e.g., differences in the national consumer protection frameworks) and how this may affect the attribution of the observed problematic practices to the three directives in scope.	New analysis and examples of national differences were added throughout the report, including in section 4.1.1.1 concerning the scale of problems, section 4.1.1.4 on enforcement (including on administrative capacities) and section 4.1.3.1 on business costs, (including costs related to national laws). Overall, the consultations and data collection did not indicate any significant differences regarding the relative scale of the explored problematic practices between Member States. New analysis was developed on enforcement, acknowledging that in the digital context, the launch of national actions using the three Directives, the use of

	certain investigative and enforcement tools, and participation in EU-wide sweeps and coordinated actions have been uneven across the Member State authorities due to multifaceted reasons, including differences in the available capacities and resources.
(8) The report should clarify to what extent insufficient enforcement reduces the effectiveness of existing regulation, including by being clearer on what insufficient enforcement in practice means and what should be considered as sufficient enforcement. In this context, the report should better assess to what extent enforcement issues with the current directives are linked to the administrative capacity issues and whether there are difference across the Member States.	Additional analysis on enforcement was added in section 4.1.1.4, expanding on key aspects of the enforcement assessment. It was clarified that for the purposes of this Fitness Check, the 'sufficiency' of enforcement is determined based on the volume and content of the court and enforcement actions that have relied on the three Directives in the digital context and qualitative stakeholder views.[178] Additional analysis of public enforcement was provided, including references to the reasons for difficulties with enforcement in digital markets, as analysed in more detail in the 2024 application report on the CPC Regulation and administrative capacity issues.
(9) The report should significantly deepen the analysis on the competitiveness and SME dimension. It should explain whether EU-based service providers, in particular SMEs, may experience a competitive disadvantage compared to their third-country competitors. It should assess whether the existing directives have affected the capacity of business to innovate, when compared to practices observed outside the EU.	A new section on competitiveness, innovation and impacts on SMEs was developed (4.1.1.2), significantly deepening the analysis on several aspects, such as explaining the overall low magnitude of the burdens imposed by the three Directives, including on SMEs, highlighting the competitiveness challenges vis-à-vis non-EU traders and the connection between innovation and consumer trust.
(10) The cost estimates should be clearly identified indicating the methods used. The simplification potential should be identified precisely. Stakeholder views should be presented in a more balanced manner throughout the report.	Additional explanations on business costs were provided in section 4.1.3.1 and Annex II, including on the calculations carried out on the basis of the data obtained from the business survey, e.g. a clearer distinction between adjustment and administrative costs, including between one-off and recurring costs. Additional analysis was provided on the costs stemming from differences in national laws when trading cross-border, although these costs were not quantified. The simplification potential was outlined more clearly in section 4.1.3.4 as a list of concrete

[178] However, no specific numeric targets are established, as this would be an arbitrary exercise, in particular taking into the account data limitations about the national court judgments and action. Quantitative court data and statistics are either not available in most Member States or do not provide a sufficient level of detail that would enable to understand the legal provisions/Directives at stake or to distinguish between online and offline scenarios.

	measures that could be further explored in a future impact assessment. Stakeholder views were presented in a more balanced manner, highlighting questions on which there were disagreements between respondents.
(11) The conclusions and lessons learned sections should be revised to accurately and objectively reflect the amended analysis fully taking into account limited robustness of underlying evidence. Overall, the report should refrain from statements about concrete measures to be taken as this is not the purpose of a Fitness Check but rather for a future impact assessment. The report should bring out more clearly lessons learned regarding the evolving EU regulatory landscape in the digital area.	Section 5 on conclusions and lessons learned was adapted to reflect the amended analysis, including on the importance of enforcement (making a link to the CPC Regulation reform), the scale of the challenges left outside of the scope of the broader digital legislation and the need to improve the monitoring processes in the EU consumer policy area. It was clarified that the Fitness Check specifically refrains from prejudging any future prioritisation of issues and the content or format of the follow-up actions. Concrete areas for improvement were highlighted to ensure a stronger, more consistent and coherent application of the broader EU digital acquis affecting consumers.

After resubmission on 1 July 2024, the RSB issued a positive with reservations opinion on 25 July 2024. The RSB's general comments were the following:

(1) The limitations of the evidence base are not sufficiently reflected in the conclusions. The lessons learned on the need to improve the monitoring and evidence collection processes are not sufficiently developed.
(2) The approach and assumptions used to estimate cost to business are not sufficiently justified.

The specific comments elaborate on these aspects. The following table explains the key issues raised by the Board and the adaptations introduced to the report.

RSB comments – What to improve	**Adaptations introduced**
(1) The report should explicitly acknowledge the limitations and uncertainties of the evidence and the sources of the data in the conclusions. The fact that the quantitative analysis is mainly founded on opinion-based data as well as the difficulties in isolating and attributing the impacts directly to the Directives and how this affects the quantitative results should be explained clearly in the main report. Any conclusions stated should not go beyond what is clearly supported by the empirical analysis. In the absence of credible analysis of attribution, the report should refrain from making statements and conclusions that imply that the attribution was established. Given the limitations, the	The limitations and uncertainties related to the evidence base are further highlighted in the conclusions in section 5 and statements on the evidence base are further qualified across the report. Notwithstanding these challenges that are not unique to this policy area, the general conclusions are deemed reliable and consistent with previous evaluations in the EU consumer law area, including the most recent evaluations, notably the 2024 application reports on the CPC Regulation and the Modernisation Directive. The conclusions present a synthesis analysis triangulating all of the data and qualitative information collected. The summary assessment of the efficiency criterion was adapted from "positive" to

report should also refrain from stating or suggesting that the evidence base is robust. The report should better explain how efficiency can be considered "positive" in light of "limited" effectiveness.	"positive with limitations". This assessment reflects the positive findings about the low cost burden of the Directives, while acknowledging that benefits are not fully realised (which has a direct link to limited effectiveness) and the challenges with attribution and quantification. With increased effectiveness, traders could reap more net benefits in the long term.
(2) The lessons learned on the need to improve the monitoring and evidence collection processes should be further developed. The report should state what data will be needed to better monitor, assess and demonstrate causality of impacts. Apart from quantitative data, the report should deepen the need assessment of qualitative data, in particular related to the factors impacting low compliance by businesses and insufficient enforcement by relevant authorities. The lessons learned should also reflect the need for a credible baseline in particular regarding indicators in order to allow for monitoring of developments. The need for evidence regarding identified problematic practices should be better developed.	Additional options for improving the monitoring and evidence collection processes were added in section 5, while acknowledging the importance of preserving the low administrative burden of these Directives and looking towards the development of automated tools. Examples of key data gaps were highlighted. It is clarified that any future evaluation or impact assessment related to the Directives in the digital context should benefit from the lessons learned in this Fitness Check, such as the formula for measuring consumer detriment that takes into account digital market growth. This Fitness Check strives to establish a baseline that can be used for monitoring developments and further built upon in the future for any new policy initiatives.
(3) The report should further explain and better justify the approach to the estimation of the cost to business. It should be clear how companies surveyed have been selected and to what extent it is possible to extrapolate the survey results to the whole digital economy considering its high heterogeneity. The approach to extrapolation should be better developed in particular given that the majority of companies indicate low costs and considering the resources deployed by the companies. The report should justify all the assumptions related to business-as-usual activities which seem to be in contradiction to the business stakeholder evidence. Given the stability of EU consumer law and the absence of reporting requirements, the report should also better explain why companies need to check	Additional information on the cost estimations and the selection of traders/sectors was provided in Annex II. An additional graph about the composition of the traders responding to the business survey was provided in Annex V. The approach and assumptions regarding the business cost assessments follow those taken in the previous 2017 Fitness Check to ensure comparability, to the extent possible. The extrapolation to the EU level on the basis of the quantitative estimates from the business survey is sufficiently reliable, since it included all types of digital economy players, ranging from online retailers selling physical goods to traders providing digital services for 'free' in exchange for consumer data. Additional information was provided on the breakdown of costs per company size.

compliance with consumer Directives annually.	It was clarified that the Directives do not require traders to conduct any annual or regular compliance checks, but some traders nevertheless report that they are diligently verifying whether their practices are compliant on a continuous basis. It is emphasised that these estimates cannot be directly attributed to the Directives and that they are likely to relate to the national legal framework, sectoral legislation and EU law beyond these Directives, as well as to national case law developments and possible national reporting obligations. Traders are not able to distinguish between such costs per Directive nor between the online vs offline environment – such activities are part of broader compliance efforts.
(4) Given that the analysis of the enforcement deficit rests mainly on the Consumer Protection Cooperation network, the report should also assess the links between national consumer protection practice and capacities and the effectiveness of the Directives. The report should analyse the costs to national authorities in particular related to inspections and complaint handling.	The analysis of enforcement deficits focuses on multiple aspects, especially the clarity of the substantive/material laws, not only the procedural frameworks for enforcement. It is explained that public enforcement by administrative authorities and through the CPC network is not the only way of enforcing the Directives in the digital context. Additional analysis on enforcement was added in section 4.1.1.4 to underline that differences in the capacities and resources between national authorities have an impact on the effectiveness of the Directives. However, the analysis remains at a general level because quantitive data on resources and administrative capacities is very limited (i.e. national authorities are unable to provide such data). Furthermore, the enforcement costs are not distinguishable per Directive, between the online or offline context, nor between different activities such as inspections and complaint handling. It was explained in section 4.1.3.3 that the responding authorities did not provide additional details on the inspection and complaint handling costs, which would enable further analysis. However, data from publicly available annual reports of three national authorities was added to illustrate the differences in the resources invested. Nevertheless, the

	data does not enable to disentangle the resources spent enforcing the Directives evaluated.
(5) Regarding the estimation of consumer detriment, the report should better explain the limitations regarding the use of perceived problems (opinion data) as a proxy for complaint incidence rate.	Additional explanations were added in section 2.2 concerning the limitations regarding the use of consumer complaints as a proxy for detriment, especially because it is likely to underestimate the real scale of infringements (e.g. many consumers do not make official complaints for various reasons). Nevertheless, consumer complaint figures have been a key indicator in the area of EU consumer protection policy to measure progress over time, alongside other sources of data. In addition, the analysis of consumer detriment was reinforced in the second submission through a calculation based on ESTAT's household survey data collected from Member States.

Evidence, sources and quality

The Fitness Check was supported by an evidence base developed in line with the Better Regulation Guidelines, through a methodology encompassing a broad range of different qualitative and quantitative data, collected over the course of two years, with support from an external study. The key evidence sources, their quality and overall methodology is further described in Annex II.

Use of external expertise

The Fitness Check report was supported by an external study – the 'Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161'. The study was carried out for DG JUST under Framework Contract JUST/2020/PR/03/0001 by the Centre for Strategy and Evaluation Services (CSES), supported by VVA (now Ernst & Young) and Tetra Tech. In addition, further organisations supported the analysis in specialist areas (WIK and LE Europe).

Additional expert consultations are further explained in the stakeholder consultation synopsis Annex V.

Annex II. Methodology and Analytical models used

The evaluation is based on a mixed-method data collection approach, combining qualitative and quantitative research methods.

The Fitness Check was supported by a methodology encompassing a broad range of different data, collected from a range of complementary sources over the course of two years, with support from an external study. The information gathered has been triangulated/cross-checked to identify points of consensus and disagreement, allowing further analysis of the reasons behind these findings. The Fitness Check complied with all of the necessary elements of the Better Regulation Guidelines, such as completing an analysis of all five evaluation criteria (effectiveness, efficiency, coherence, relevance, EU added value), allocating sufficient time for the evaluation process, looking at simplification and burden-reduction potential as part of the efficiency analysis, conducting broad consultations of all relevant stakeholders and examining possible regulatory overlaps, inconsistencies and synergies across the broader EU regulatory framework applicable to the digital environment.

Key evidence sources used include:

- a **call for evidence** which received 71 responses from 14 Member States and the UK. It covered a broad spectrum of stakeholders (e.g. citizens, business associations, companies, non-governmental organisations, a consumer organisation, public authorities, online platforms and other) and sectors (from airlines to food delivery services).
- a **public consultation** which received 369 responses and 71 position papers. Most responses (95%) came from EU countries, notably from Portugal, Belgium, Germany, Italy and Spain, while 5% came from non-EU countries. It covered a broad spectrum of stakeholders (e.g. citizens, business associations, companies, non-governmental organisations, a consumer organisation, public authorities, online platforms and other) and sectors (including the largest tech companies such as Meta, Alphabet, Amazon and Apple).
- three additional **major surveys**:
  1) **Consumer survey** of **10 000 consumers** across 10 Member States. The same 10 Member States were used for the consumer survey, business survey and sweeps (DE, EE, ES, FR, IT, HU, PL, PT, RO, SE), allowing the different results to be cross-referenced and/or complement each other. This consumer survey complements the Commission's biennial Consumer Conditions Scoreboard (sample size 27 000 consumers across EU27) with more detailed questions. The 10 Member States were chosen to be representative in terms of sample size, covering different EU regions and allowing, to the extent possible, extrapolation to the EU. The consumer and business surveys were applied to a statistically representative sample that enables a high degree of statistical certitude. Furthermore, it was possible to distinguish between respondents based on a variety of factors, such as the presence of health problems, impulsiveness, risk preferences, internet addiction, gambling tendencies, confidence in using digital tools and trust in online traders.
  A pre-established large-scale panel was chosen to achieve a high survey response with strong representativeness according to different parameters, such as geographic coverage, age and gender. The consumer panel was coordinated by

VVA Market Research, using a structured Computer Assisted Web Interview (CAWI) survey, carried out in June and July 2023 through the Cint platform of consumer panels, a network of proprietary and third-party panels that brings together more than 149 million people from over 130 countries worldwide. All panels are pre-recruited groups of people who have agreed to participate in online research (surveys/polls/ad testing). The recruitment process includes 2 steps. The first step involves becoming a member of a country panel. Cint recruits panellists using: Direct email/newsletter send out, Pop-Ups & Banners, Loyalty websites, Social Media, Offline/online advertisement, Telephone and Face-to-face based recruitment. All Cint panels and panellists are subject to the same quality standards and quality checks. The second step of the recruitment process is related to the sample size and respondents of the survey. VVA launched the recruitment through Cint's panels in the respective countries. An email and/or push notification was sent to all relevant panellists who are part of the target sample. Every email includes an invitation link to access the survey. All respondents were asked at the beginning of the survey some screening questions to ensure that the sample of respondents is representative of the general population of each respective country (based on quotas for age, gender and geographical location). The final sample achieved was aligned with the general population so there was no need to apply any weights.

2) **Business survey** of **1000 companies, including 77% SMEs** across 10 Member States. As there was no pre-established test panel among businesses covering the EU, a high survey response was ensured by working with an external provider of Computer Assisted Telephone Interviewing (CATI panel) able to construct business panels according to the specified parameters to ensure representativeness in terms of geographic coverage, company size (micro, small, medium and large) and sector of activity. The main purpose of a dedicated business survey was to gather views from SMEs and to estimate the business costs that they face when complying with the rules in the digital environment. The survey included a filtering question to ensure that the trader provides products or services directly to consumers through a website, app or online platform/marketplace.

3) **Targeted stakeholder survey** of 164 stakeholders, which included more detailed and technical questions than those in the public consultation. The targeted survey was carried out through the CSES' online survey platform and aimed at well-informed stakeholders with a good understanding of the EU consumer law framework and its application in the digital environment (e.g. ministries responsible for consumer policy and legal transposition, enforcement authorities, consumer organisations, traders and their representative associations).

- 101 **interviews,** including with leading academics and key stakeholders in this area. The interviews complemented each other and were used to validate the findings from the desk research and surveys. They also made it possible to obtain granular feedback on the evaluation questions and issues across different research topics.
- compliance-check **sweeps** covering 10 different categories of consumer law obligations across **300+ websites/apps** involving traders from 10 Member States (the same Member States as in the consumer and business surveys) to complement the data received from the annual sweeps conducted by the Consumer Protection Cooperation (CPC) network of consumer protection authorities in targeted areas. The selection of websites and apps depended primarily on the specifics of the relevant topic that was investigated and their relative importance (e.g. volume of traffic per month in each country covered; ranking of video game popularity on a gaming platform), covering marketplaces, e-commerce sites, travel and

accommodation, social media, search engines, dating, gambling, video games, price comparison sites etc. Several topics were selected specifically for checking compliance with new provisions introduced by the MD. The methodology consisted of researchers using a 'scenario-based cognitive walkthrough' method, which involves taking on the persona of an end-user/consumer. For the purpose of this type of mystery shopping, the use of professional researchers was preferred over regular consumers, given the complexity of the problematic practices deployed and the specificity of the applicable legal provisions. The role of researchers was carried out by experts involved in other data collection activities, who would be more familiar with the subject matter at stake and the main issues in their respective countries. It was considered that automated data collection may not be suitable for assessing all of the research topics and checking compliance with legal obligations. While some degree of automation was used (e.g. checking for unfair contract terms), manual checking by researchers was necessary in all cases to validate the results and incorporate evaluative judgment.

- extensive **desk research** of all relevant secondary data sources from the last 5 years, including research building on several **comprehensive studies**, such as the European Parliament's studies into loot boxes, influencer marketing and personalised pricing, and the Commission's studies into digital advertising (DG CNECT, 2023) and dark patterns (DG JUST, 2022).
- comprehensive **case studies** by the contractor and additional analysis by the Commission of the most important problematic practices. Given the broad range of subjects covered by the Fitness Check, the contractor carried out more in-depth assessment of the following topics through 8 case studies: 1) aggressive practices, 2) consumer vulnerability, 3) online subscriptions, 4) personalised advertising, 5) personalised pricing and offers, 6) digital addiction, 7) social commerce and social media influencers, 8) unfair contract terms in a digital context. The case studies provided an opportunity to investigate these problematic practices in-depth, together with additional desk research and interviews conducted with experts in the field. The case studies are significant in size (each topic was subject of a separate full-length case study) and presented as an annex to the supporting study. The Commission's assessment of problematic practices in Annex VI of the FC report is a condensed analysis, building on all sources of data.
- extensive new **legal analysis** of the Directives and their interplay with new digital legislation (developed in a dynamic manner in parallel to the final adoption of instruments such as the AI Act).
- consultation of **Member State and stakeholder expert groups**, as well as dedicated **public events** like the Annual Digital Consumer Event, organised three years in a row to gather more feedback.

The quality of the evidence base should be seen in the context of various **objective limitations**:

- The **degree to which the evidence gathered in the EU consumer policy area is qualitative, primarily opinion-based**, with the usual limitations and uncertainties associated to this type of data. The reliance on Commission-run surveys is necessary due to the absence of reporting requirements in the Directives and the lack of longitudinal datasets from public or private sources (e.g. limited market sweeps by authorities; no automated monitoring solutions) on the very wide range of issues covered by the Directives' material scope. In terms of survey limitations, it is noted that the targeted stakeholder survey was more industry-dominated, with

over 50% of participants representing traders or trade associations. Furthermore, the public consultation generally cannot be considered to be a representative survey, in particular due to its sample size. However, representative views were obtained through the consumer survey and business survey, which cover a sufficient sample size, ensuring geographical balance and the possibility to extrapolate to the EU. In the report, there is a conscious balance between using data from the different surveys, to ensure neutrality. Furthermore, questions on which there was major divergence among respondents have been outlined in the report. The report did not rely on the consumer survey or consumer responses to the public consultation as regards legal assessment questions.

- The **limited availability of appropriate quantitative data, in particular as regards the ability to measure progress over time.** For example, whilst the findings of the different surveys conducted as part of this Fitness Check enabled to estimate the current (2023) consumer detriment in relation to problematic digital practices (including in quantitative terms), there do not exist specific detriment figures specifically about the application of the three Directives in the digital context at the start of the evaluation period (2017). In order to ensure a robust description of the scale and development of the problems, the consumer complaints and detriment figures from 2017 were put into the context of e-commerce growth, among other factors. Additional sources of data about consumer detriment were sought out and used by analogy. Similar considerations applied for measuring the evolution of specific problematic practices. For example, while some of the practices already existed at the start of the evaluation period (e.g. influencer marketing, dark patterns), others emerged only recently (use of AI chatbots) in B2C markets.
- The objective **difficulty of attributing the benefits and costs to the specific rights and obligations stemming from the three Directives**. While stakeholder feedback gathered for the purpose of this Fitness Check clearly points to a strong link between the application of the three Directives and the effectiveness of consumer protection in the digital environment[179], it is not possible to directly attribute all of these changes to the Directives. To reduce administrative costs, the Directives do not include any reporting requirements for traders or Member States (beyond the standard requirement to notify the Commission of the national transposition rules). EU businesses therefore do not have customised accounting systems regarding their costs for benefits and we have to rely on the estimates provided during interviews. For example, when examining business costs, multi-channel traders found it difficult to disentangle compliance costs associated with digital channels from offline channels and most traders are unable to isolate costs for their obligations regarding the three Directives specifically from those concerning for example product labelling or safety requirements. As a result, the estimates given by traders are also likely to include national legislation going beyond EU consumer law requirements as well as certain EU sector-specific legislation and its national implementing legislation.

[179] Qualitative evidence from surveys shows that the presence of a strong regulatory framework has contributed to increasing consumer trust and creating a more level playing field for traders. Stakeholder and Member State views pointed at very positive perceptions of the contribution of the three Directives towards objectives such as ensuring a high level of consumer protection (in the public consultation, e.g. 71% identified a positive impact on protecting against unfair commercial practices). Furthermore, there was consensus among respondents about the necessity of having a strong and harmonised consumer protection framework in place in order to facilitate the functioning of the digital single market (in the public consultation, 96% agreed or strongly agreed with this assertion).

- The **lack of previous Impact Assessments and precise monitoring indicators** relevant for the three Directives in the digital context – the UCTD and UCPD pre-date the Better Regulation guidelines and were not accompanied by Impact Assessments with monitoring indicators for their objectives. The 2008 Impact Assessment accompanying the CRD did not include monitoring indicators and the material scope of the proposed Directive changed significantly in the course of legislative negotiations. As a result, there are limitations regarding the lack of comprehensive baseline data or information, for example about the one-off compliance costs. Furthermore, as the Directives apply to both online and offline environments, there are limitations regarding the extent to which it is possible to disentangle the 'digital' impacts and costs. A digital-specific intervention logic, baseline and indicators had to be developed retroactively for the purposes of this Fitness Check.
- The **limitations regarding data collection at European and national level concerning the amount of consumer complaints, case law and enforcement activities**. As a result, the estimates given in this Fitness Check are likely to underestimate the scale of the problems. Quantitative court data and statistics are either not available in most Member States or do not provide a sufficient level of detail that would enable to understand the legal provisions/Directives at stake or to distinguish between online and offline scenarios. Available data sources used in the evaluation included representative surveys, interviews, desk research, data from the European Consumer Centre Network about cross-border complaints, data from the Online Dispute Resolution platform about complaints concerning goods or services bought online and data about the CPC network's coordinated actions and alerts.

The assumptions and limitations related to data collection and analytical tools are further explained in the supporting study and aligned with the requirements of the Better Regulation Guidelines and the accompanying Toolbox. The external contractor took additional measures to ensure internal and external quality assurance.

Additional information about calculations of business costs

Concerning the estimation of **business costs** related to applying the three Directives in the digital environment, there are a number of assumptions and considerations taken into account by the external contractor. The first concerns the number of companies affected, which was estimated at 1.3m. This figure includes online retailers engaging in B2C sales in the EU market, estimated at 1.254m, in addition to approximately 10 000 traders participating in the online platform economy and 28 000 traders offering digital subscriptions.

Traders that face compliance costs with EU consumer law in the digital environment include sellers engaging in e-commerce, online marketplaces, online platforms as well as new types of traders, such as professional social media influencers. The nature and degree of the costs vary greatly between traders, given the different requirements they face and depending on whether they engage in the online sale of physical goods, provide digital content or services, advertising, intermediation or engage in other commercial practices. For instance, costs regarding some of the information disclosure requirements introduced by the MD are only faced by online platforms and marketplaces (e.g. disclosure of search ranking parameters), whereas most information obligations apply to all traders, regardless of their business model. Furthermore, the UCPD and UCTD contain principle-based

provisions, which means that they do not necessarily prescribe detailed requirements but require traders to act in accordance with principles of good faith, transparency and due diligence towards consumers. Moreover, there are only a limited number of digital-only provisions in the three Directives, whereas most provisions apply to both online and offline environments.

Another relevant consideration is the distinction between rules stemming directly from the Directives and those stemming from additional national laws, especially in the case of minimum harmonisation in the UCTD (e.g. additional costs of complying with national blacklists of unfair contract terms). Furthermore, in estimating the costs, a discount can be made when considering the 'business as usual' costs that traders would incur regardless of the obligations in the Directives. For example, 'business as usual' costs are costs that would have been incurred anyway by traders regardless of whether there are information obligations in place due to EU consumer law. These enable a discount to be made in terms of estimating the difference between the gross and net costs of compliance.

Finally, as the Directives have been in place for over a decade, the initial familiarisation costs are only relevant to traders that apply EU consumer law for the first time or in case of new amendments to the Directives, e.g. by the MD or DMFSD. Many traders operating e-commerce websites will already be familiar with the application of EU consumer law through offline sales channels. Therefore, familiarisation costs with the legislation (and specific information requirements for traders) are likely to be negligible for traders operating in a multi-channel environment as they are already experienced in applying the legislation. Notwithstanding, there will be new one-off compliance costs for traders that operate digital only, an increasing trend in the past decade for some apps and websites. However, based on Eurostat data, it is estimated that less than a quarter (22.8%) of traders operate online only. Familiarisation costs are likely to be relevant mainly to this group, i.e. traders that are digital only and applying EU consumer law for the first time.

The overall approach and assumptions for the business cost estimations were the same as in the earlier 2017 Fitness Check in order to ensure comparability to the extent possible. As it is not feasible to cover all business sectors in the analysis, a selection of sectors was provided. For comparison, the 2017 Fitness Check selected five sectors (large household appliances, electronic and ICT products, gas and electricity services, telecommunication services, pre-packaged food). This time, the focus was on traders which provide products or services in the online environment, while also ensuring some sectoral continuity with the 2017 Fitness Check by including some traditional sectors which engage in both online and offline sales. The sectors chosen were the following (with NACE codes - the Statistical Classification of Economic Activities in the European Community - where available): social media platforms, individual e-commerce firms, online marketplaces, app developers, e-commerce website developers, digital service providers, manufacture of computer, electronic and optical products (C26), manufacture of electrical equipment (C27), retail sale via mail order houses or via Internet (4791), retail sale of information and communication equipment in specialised stores (474), retail sale of computers, peripheral units and software in specialised stores (4741), retail sale of telecommunications equipment in specialised stores (4742), retail sale of audio and video equipment in specialised stores (4743), telecommunications (J61). Data and qualitative information on costs covering these sectors was sought through the interview programme, business survey and targeted survey. The primary data collection source for quantitative figures on costs was the business survey, although additional complementary insights were also gathered through the targeted survey.

The estimations of the costs establish a range - the first cost figure relates to traders that have dealt with managing compliance in-house ('lower bound'). The second higher figure relates to traders that have used a combination of in-house resources and external expertise (e.g. legal services, professional advice) ('higher bound').

Adjustment costs	**Administrative costs**
There are a total number of 130,000 companies (10%) affected by 'high costs' of familiarisation and adjusting to the legislation. The median number of employees and days of companies that reported costs are 2 employees and 20 days in a year per employee. It is expected that existing employees will include these activities as part of their everyday activities and not likely to spend a full day on familiarisation and adjustment. The average hourly wage in 2022 was estimated at 30.5 EUR/hr (according to Eurostat figures). Assuming each employee spends 1.25hours a day, the total cost per company can be estimated at c. EUR 1,600 (2 employees x 20 days per employee x 1.25hours/day x EUR 30.5/hr; rounded up). Should more hours be needed per employee, the median costs of external services could still be used as a lower bound. The total adjustment costs, including familiarisation costs, across all companies are estimated at EUR 208m (130,000companies*1600 EUR/company). If a higher average value were to be assumed of the adjustment costs - EUR 2,331 including the average costs of hiring external services - then total costs would increase to EUR 303m annually.	There are a total number of 195,000 companies (15%) affected by 'high costs' of checking compliance with the legislation. The median number of employees and days of companies that reported costs are 2 employees and 21 days in a year per employee. It is expected that existing employees will include these activities as part of their everyday activities and not likely to spend a full day on checking compliance. The average hourly wage in 2022 was estimated at 30.5 EUR/hr (according to Eurostat figures). Assuming each employee spends 1 hours a day[180], the total cost per company can be estimated at c. EUR 1,280 (*2 employees x 21 days per employee x 1 hour/day x EUR 30.5/hr).* The total costs of checking and ensuring compliance across all companies are estimated at EUR 249.8m (195,000companies*1280 EUR/company). If a higher average value were to be assumed for the administrative costs - EUR 2,500 including the average costs of hiring external services - then total costs would increase to EUR 487.5m annually.

Additional information about calculations of consumer complaints and detriment

The representative consumer survey was used to collect quantitative data about the financial detriment suffered by consumers as a result of the problems experienced. When presenting the figures, median numbers are used - the difference between the average and the median reflects the high variation in the costs experienced by consumers as consumer

[180] We have assumed a bit less time in checking compliance per day per employee assuming they are already familiar with the legislation.

detriment. The median is less affected by outliers and skewed data than the mean and is usually the preferred measure of central tendency when the distribution is not symmetrical. The survey results show that 41% of consumers ended up over-paying or experiencing extra charges as a result of a problem (median amount estimated at EUR 35). The median costs to consumers of repairs or replacement were estimated at EUR 30, the costs of dispute resolution or court proceedings were estimated at EUR 40, the costs of experts' advice were EUR 40 for those that sought advice. There were other additional costs such as phone call, postage and travel costs reported, estimated at EUR 20. As a result of their dispute resolution efforts, consumers received EUR 50 of compensation. To calculate the overall amount of detriment, two values can be presented: a cost of detriment, pre-redress, that includes extra charges and costs of repairs estimated at EUR 65, and a cost of detriment, post-redress, that includes all costs (e.g. costs of dispute resolution and expert advice but also the reimbursement) estimated at EUR 115.

Table 9 – Quantification of the amount of consumer detriment suffered as a result of problematic practices

	Average	**Median**
Price paid for products (EUR)	245	50
1. Extra charges as result of problem	137	35
2. Costs of repairs or replacement at your own expense	161	30
3. Costs of dispute resolution	214	40
4. Costs of experts advice	208	40
5. Extra costs	159	20
6. Reimbursement	251	50
Total costs of detriment (1+2) ***pre-redress (EUR)***	298	**65**
Total costs of detriment (1+2+3+4+5 -6) ***post-redress (EUR)***	628	**115**

Source: Consumer survey to support the Fitness Check

In order to extrapolate to the EU level, estimate the pre- and post-redress financial detriment at different times over the evaluation period and establish a baseline, the following formula was applied:

$$Financial\ Detriment_{year} = Total\ number\ of\ consumers\ \times$$
$$Percentage\ of\ all\ consumers\ with\ last\ internet\ online\ purchase\ in\ the\ last\ 3\ months_{year}\ \times$$
$$Complaint's\ incidence\ rate_{year}\ \times Individual\ Consumer\ Detriment_{year}$$

The various data points used for these calculations come from Eurostat and the Consumer Conditions Survey (CCS), with the latter conducted on a biennial basis, therefore estimates can only be provided for every two years. The table below applies the formula to see how the detriment experienced by consumers who purchase online evolved over the evaluation period. The estimated monetary value of consumer detriment comes from the consumer survey, as explained in the table above. For the purposes of the calculations, the number of consumers in the EU is estimated at approximately 440 million.

Table 10 - Extrapolation to the EU27 of consumer detriment suffered as a result of problematic practices over the evaluation period

European Union - 27 countries	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Percentage of all individuals with last internet online purchase in the last 3 months[181]	40.7 %	43.7 %	45.8 %	49.0 %	53.8 %	56.9 %	56.0 %	40.7 %
Complaint's incidence rate[182]	24.0 %[183]		24.2 %		27.0 %		29.6 %	
Inflation[184]		1.6%	1.8%	1.4%	0.7%	2.9%	9.2%	
Total cost of detriment pre-redress per problem experienced, median (EUR)[185]	52	52	53	54	54	56	61	65
Total cost of detriment post-redress per problem experienced, median (EUR)[186]	91	93	94	96	96	99	108	115
Pre-Redress Financial Detriment estimate, billion (EUR)	**2.2**		**2.6**		**3.5**		**4.5**	
Post-Redress Financial Detriment estimate, billion (EUR)	**3.9**		**4.6**		**6.1**		**7.9**	

Source: DG JUST, estimations based on Eurostat and CCS data

Overall, there has been an increase of consumer detriment over the evaluation period, even after taking into account inflation and e-commerce growth. The post-redress financial detriment stood at EUR 3.9 billion in 2016 before the evaluation period and is currently estimated at EUR 7.9 billion (based on the latest available 2022 data).

Additional studies

In addition to the supporting study, European institutions commissioned or supported different studies related to consumer protection in the digital environment, which were taken into account in the Fitness Check. A full bibliography of all relevant sources can be found in the Annexes of the supporting study.

Studies from the European Commission:

- Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers (2023)
- Understanding the value of a European video games society (2023)

[181] Eurostat - Internet purchases by individuals (until 2019) - isoc_ec_ibuy
Eurostat - Internet purchases by individuals (2020 onwards) - isoc_ec_ib20
[182] Consumer Conditions Survey, Q15. In the past 12 months, have you experienced any problem when buying or using any goods or services in your country where you thought you had a legitimate cause for complaint? Yes 'Total of those that purchased online in the last 12 months' (%).
[183] Results for 2016 are estimated to account for changes to the weighting of survey results introduced in 2018.
[184] Eurostat - Harmonised index of consumer prices (HICP) - annual data (average index and rate of change)
[185] Consumer survey to support the Fitness Check, figures until 2023 are deflated using the harmonised index of consumer prices (HICP).
[186] Consumer survey to support the Fitness Check, figures until 2023 are deflated using the HICP.

- Foresight on Demand (FoD): Impact of the COVID-19 pandemic on European Consumer Behaviour - Foresight Study (2023)
- Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation (2022)
- Survey on fraud and scams experienced by consumers (2020)
- Behavioural study on advertising and marketing practices in travel booking websites and apps (2020)
- Consumer market study on online market segmentation through personalised pricing/offers in the European Union (2018)
- Behavioural study on advertising and marketing practices in social media (2018)
- Behavioural study on transparency in online platforms (2018)
- Study on measuring consumer detriment in the European Union (2017)
- Study on consumers' attitudes towards Terms and Conditions (T&Cs) (2016)
- Understanding consumer vulnerability in the EU's key markets (2016)
- Study on the impact of marketing through social media, online games and mobile applications on children's behaviour (2016)

Studies from the European Parliament:

- Metaverse (2023)
- Personalised pricing (2022)
- The impact of influencers on advertising and consumer protection in the Single Market (2022)
- Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice (2021)
- Update the Unfair Contract Terms directive for digital services (2021)
- Regulating targeted and behavioural advertising in digital services: How to ensure users' informed consent (2021)
- Loot boxes in online games and their effect on consumers, in particular young consumers (2020)
- New aspects and challenges in consumer protection: Digital services and artificial intelligence (2020)
- Artificial Intelligence (AI): new developments and innovations applied to e-commerce: Challenges to the functioning of the Internal Market (2020)

Annex III. Evaluation matrix

Evaluation Questions	Sub-questions	Indicators	Data sources
Evaluation criteria – Effectiveness			
1. How successful have the Directives been in achieving or progressing towards their objectives in the digital environment?	- Have the objectives already been met? - What are the main reasons for the objectives being met or conversely not being met, if applicable? - What are the main legal provisions that have contributed towards an improved level of consumer protection and trust in the digital environment? - To what extent have these elements contributed towards an improved level of consumer protection? - To what extent have these elements contributed towards the proper functioning of the internal market through the harmonisation of laws? - Which elements are hindering improved consumer protection in the digital area?	- Extent of progress towards objectives in the digital environment. - Stakeholder perceptions on the effectiveness of the Directives. - Contribution made by the Modernisation Directive to amending the three Directives in terms of improving the digital environment. - Hierarchy of factors identified, as perceived by different stakeholders and as described in the literature. - Extent of impact on consumer protection and consumer trust. - Extent of harmonisation/creation of a level playing field for traders.	- Desk research - Interview programme - Sweeps - Public consultation - Targeted survey - Consumer survey - Business survey - Case studies - Analysis of input and output data before and after the implementation of the Directives - Examples of public and private enforcement actions at EU and national level

Evaluation Questions	Sub-questions	Indicators	Data sources
		- Number of consumer complaints and enforcement actions. - Perceptions of remaining or emerging regulatory fragmentation in the areas regulated by the Directives.	
2. Has there been an increase of problematic digital business-to-consumer practices that challenge the effectiveness of the Directives?	- Which practices are considered problematic? - Which types of traders and market sectors are making the most use of problematic practices? - Can any differences between EU Member States/regions or EU and non-EU traders be observed in this regard? - What problems do consumers face with dark patterns which are not already sufficiently addressed by the Directives or other legislation? - What problems do consumers face with social media commerce, in particular with influencer marketing? Are the existing provisions in the UCPD successful in regulating hidden advertising and other problems? Is social commerce (direct selling through social media) sufficiently addressed by the existing laws? - What transparency and fairness problems do consumers face with business-to-consumer personalisation practices (e.g. personalised advertising, offers, pricing, search results) that are not sufficiently addressed by existing legislation? - Are subscription contracts adequately addressed by either the CRD, UCTD or other EU laws?	- Extent of increase in problematic digital B2C practices and perceptions of their problematic nature. - Impact of problematic digital B2C practices on consumer welfare. - Perceptions regarding the degree of protection afforded by the current framework. - Degree to which other regulations address the identified problems. - Extent to which dominant approaches taken by market players are perceived as problematic. - Stakeholder perceptions of extent to which UCPD blacklist prohibitions are able to capture current problematic digital practices.	

Evaluation Questions	Sub-questions	Indicators	Data sources
	- What are the main approaches followed by traders with respect to the procedure for termination by the consumer of contracts for digital content or services? Is it technically difficult for consumers to terminate a contract for any goods or services purchased through the digital means? - What are the main market practices for the marketing and use of intermediate virtual currency as part of, or in relation to, the provision of digital content and services and what problems do consumers face? To what extent is sufficient information provided to consumers regarding the use of virtual currency and virtual items? - How successful has the UCTD been in protecting consumers against unfair contract terms in the digital environment in terms of fairness and transparency? - What are the types of contract terms that may put consumers in a disadvantageous position vis-à-vis traders in the digital environment? Is the current indicative list of potentially unfair terms (Annex to the UCTD) successful in capturing them?	- Examples of specific problematic practices which are insufficiently covered.	
3. Are there any market and/ or technological developments that are likely to challenge the effectiveness of the Directives in the future?	- What impact will digitalisation and the use of specific technologies have on the effectiveness of the Directives? - What impact might specific new technologies and/ or types of contracts have (e.g. the use of smart contracts, increase in personalisation, impact of AI,	- Stakeholder perceptions of impact of new technologies on the effectiveness of the Directives. - Extent that primary and secondary desk research evidence indicate that market	

Evaluation Questions	Sub-questions	Indicators	Data sources
	use of IoT, connecting data from different sources, including social media)?	developments jeopardise the effectiveness of the Directives going forward.	
4. Are there legal gaps or uncertainty/grey areas in the Directives with regard to addressing problematic digital practices?	- Which of the problematic practices (highlighted in the previous evaluation questions) are likely to already be considered illegal under the existing rules and only require improved enforcement? - Are the concepts of 'average consumer' and 'vulnerable consumer' still fit for purpose? - How successful is the UCPD in addressing 'digital asymmetry' and situational vulnerabilities? - Is the concept of 'transactional decision' (Article 2(k) UCPD) successful in capturing all relevant decisions by the consumer, such as interacting with digital content (e.g. scrolling, liking, sharing, clicking)? - Do the Directives ensure the prevention of the potential negative effects on the social and financial situation of consumers due to addiction and prolonged use of certain digital content and services? - Are the current blacklist prohibitions (Annex I to the UCPD) successful in capturing problematic digital practices? - Are the provisions on aggressive practices (Articles 8 and 9 UCPD) sufficiently precise and successful in capturing problematic digital practices?	- Legal analysis of the Directives and the Commission's interpretative Guidance. - Stakeholders perceptions about the identified gaps or legal uncertainties/grey areas. - Extent to which specific provisions have been used in public and private enforcement actions. - Stakeholder perceptions of effectiveness of the Directives in preventing the exploitation of consumer vulnerabilities, including practices targeted to consumers with fewer digital skills, children, consumers with mental or physical infirmity, addictions etc.	

Evaluation Questions	Sub-questions	Indicators	Data sources
	- Are the current indicative unfair terms (Annex to the UCTD) successful in capturing unfair terms used in the digital environment?		
5. What is the level of business compliance with the Directives and how effective has public and private enforcement been in the digital area?	- To what extent is compliance with the Directives enforced at national level? - How effective are mechanisms for addressing non-compliance? - What problems do traders, including in particular SMEs, face in complying with the Directives? - What hinders/influences effective enforcement in the digital area? - Are the current rules on the burden of proof and the obligation to provide evidence (Art. 12 UCPD) functioning adequately in the digital area? Are there national differences in the approach to burden of proof rules? - What are the consequences (e.g. assumption of non-compliance) for the failure to provide evidence?	- Estimated level of business compliance. - Stakeholder perceptions of effectiveness of enforcement in the digital area. - Extent to which this is confirmed in desk research conducted. - Analysis of availability, awareness and ease-of-use of enforcement measures for consumers and SMEs. - Industry and consumer associations' views on whether industry (particularly SMEs) is compliant and assessment of the impact of non-compliance. - Stakeholder perceptions as to whether the existing rules on the burden of proof are creating disproportionate barriers.	
Efficiency			
6. What are the regulatory costs of the Directives for the different actors involved	- What is the economic cost for businesses to comply with the Directives, including specifically for SMEs taking into account the weight of the	- Cost-benefit assessment based on the data gathered.	- Desk research - Interview programme

Evaluation Questions	Sub-questions	Indicators	Data sources
(Member States authorities, businesses, consumers) and for the society overall, in the digital area, including consumer detriment?	different kinds of SMEs operating in the digital sector? - How do these costs compare to the costs of other EU legislation that addresses problematic digital practices? - To what extent have consumers been affected by the non-compliance with the Directives with regard to the digital area? What is the size of consumer detriment? - To what extent are these costs proportionate to the benefits, assessing first within each stakeholder category and as a second step, the overall effect for society?	- Level of direct cost and degree of indirect cost associated with implementation of the Directives. - Degree to which cost levels are the same or lower than other EU legislation addressing problematic digital practices, and do not overlap other requirements. - Comparison to the 2017 Fitness Check of EU consumer law (covering both online and offline environments). - Estimation of the size of the consumer detriment. - Degree to which benefits outweigh costs based on quantitative assessment (to the extent possible) and stakeholder perceptions.	- Public consultation - Qualitative and quantitative figures on consumer detriment from the consumer survey and additional studies - Qualitative and quantitative figures on costs from the targeted survey and business survey - Case studies
7. What are the benefits of the Directives for the different actors involved (Member States authorities, businesses, consumers) and for the society overall, in the digital area?	- What is the impact of the benefits derived from the Directives? - To what extent do the Directives limit illegal or unethical activities that consumers face in the digital environment? - To what extent do the Directives create a level playing field for traders through the harmonisation of laws?	- Degree to which the Directives improve consumer trust and consumer welfare, support cross-border trade and the digital single market, and limit problematic practices.	

Evaluation Questions	Sub-questions	Indicators	Data sources
8. To what extent are there any areas where there is potential to reduce inefficiencies, particularly regulatory burden and to simplify their application with respect to the digital environment?	- In which areas is there scope for reducing inefficiencies, particularly regulatory burden? - Is there information overload for consumers and, if so, how to address it? - What opportunities are there to reduce costs for businesses as regards the obligations for the provision of pre-contractual information to consumers in relation to contracts for digital content and services? - What opportunities are there to reduce costs for businesses to comply with the right of withdrawal in the CRD in relation to contracts for digital content and services?	- Comparison of costs vs benefits for existing rules compared with possible alternatives. - Degree to which the same or improved outcomes could be achieved through less costly and/or burdensome rules. - Extent to which cost reduction impacts the provision of pre-contractual information.	
Relevance			
9. To what extent do the initial objectives of the Directives still correspond to the current needs of consumers in the digital area and how well adapted are they to market trends (e.g. AI, personalisation, IoT)?	- Do the three Directives demonstrate ongoing regulatory fitness for purpose in light of digitalisation? - To what extent are the Directives addressing the current needs for protection and preventing the exploitation of consumer vulnerabilities in the digital environment? - Is it necessary to amend the concepts of the Directives to cover digital asymmetries? - Is it necessary to amend the concepts of 'average consumer' and/or 'vulnerable consumer'? - To what extent is the wording of Article 5(3) UCPD – listing types of vulnerable groups (mental or physical infirmity, age/children or credulity), broad enough to cover all types of relevant vulnerable	- Degree to which the Directives can meet current and future objectives, taking into account expected technological developments. - Degree to which the issues and objectives addressed by the Directives remain relevant today and in the foreseeable future. - Degree to which the Directives would continue to meet their objectives in a scenario with increasing use of personalisation, reliance on AI, automated contracting etc.	- Desk research - Interview programme - Public consultation - Targeted survey - Consumer survey - Business survey - Case studies - Analysis of assessment of effectiveness

Evaluation Questions	Sub-questions	Indicators	Data sources
	groups (e.g. people with less digital skills) and different types of situational vulnerabilities?	- Evidence of gaps and shortcomings in the application of the general concepts in the Directives that undermine consumer protection. - Stakeholder perception on the need to amend the general concepts in the Directives.	
10. To what extent do the issues addressed by the Directives continue to require action at EU level to ensure high level of consumer protection in the digital area?	- Is it necessary to introduce new obligations and prohibitions regarding dark patterns that are not already expressly regulated in the UCPD or other EU interventions, such as the DSA? - Is it necessary to introduce a 'fairness by design'/neutral interface design obligation? - Is it necessary to introduce an express prohibition of exploiting personal vulnerabilities or psychographic profiling to exercise emotional or psychological pressure with the aim or effect of distorting a consumer's transactional decision? - Is it necessary to introduce new obligations specifically regarding influencer marketing and social commerce more broadly? - Is it necessary to introduce additional transparency obligations about personalised practices? Is it necessary to further regulate the parameters on which the personalised commercial practice was based, in particular data about vulnerabilities? Is it necessary to introduce an option of non-personalisation? By default?	- Legal analysis of the Directives (with reference to the effectiveness and coherence analysis). - Extent to which the identified issues are covered by other EU interventions. - Evidence of potential solutions to address the problems and meet objectives. - Stakeholder perceptions regarding the need for amendments and degree of support for potential solutions. - Evidence of shortcomings in the application of Directives to the issues identified, such as dark patterns, aggressive practices, social commerce, influencer marketing, personalisation	

Evaluation Questions	Sub-questions	Indicators	Data sources
	- Do the requirements for the provision of pre-contractual information in the CRD correspond to the current needs of consumers in the digital area, including the manner in which the pre-contractual information is presented? - Is it necessary to introduce specific rules for the termination of contracts or regarding the length and renewal of subscription contracts for digital services concluded between traders and consumers? - Is it necessary to introduce specific rules that aim to mitigate the potential negative effects on the social and financial situation of consumers due to addiction and prolonged use of certain digital content and services? - Is it necessary to add new terms to the indicative list of unfair terms (Annex to the UCTD) or to introduce a blacklist? Is it necessary to otherwise adapt the existing provisions of the UCTD to better address the imbalances resulting from the use of data-driven personalisation practices?	practices, unfair terms, scalping practices, addictive design etc.	
Coherence			
11. Are there any internal discrepancies, inconsistencies or complementarities between the provisions of the Directives related to transactions and practices in	- To what extent and how do the provisions and activities of the three Directives address similar topics (e.g. information provision)? - To what extent and how are the activities in the areas regulated by the Directives coherent and complementary? Or, conversely, incoherent and inconsistent?	- Examples of scenarios where the applicable rules result in discrepancies, inconsistencies or complementarities, per focus topic. - Degree to which the discrepancies, inconsistencies or	- Desk research - Interview programme - Public consultation - Targeted survey - Case studies

Evaluation Questions	Sub-questions	Indicators	Data sources
the digital environment? (internal coherence)		complementarities identified impact the coherence of the EU legal framework.	
12. Are there any internal discrepancies, inconsistencies or complementarities between the Directives and any other EU legislation with similar objectives, such as the DSA, DMA, AI Act, GDPR, AVMSD and Data Act? (external coherence)	- In what areas and how do the provisions of the three Directives address similar digital market issues to existing and emerging EU legislation? - To what extent and how are any of the identified interfaces having an impact on the overall regulatory fitness for purpose of the EU legal framework? - How far does the advent of other digitally focused EU legislation influence the overall coherence of the EU legal framework? - Is there evidence of inconsistencies in the way the Directives and other relevant EU law regulate consumer protection issues in the digital environment? - Is there a need to strengthen coherence of the three Directives with other EU legislation through legislative amendments or other action? - To what extent is the UCPD coherent with other EU interventions, such as the DSA, on topics such as the obligations of online platforms, dark patterns, recommendation systems and online advertising? - To what extent is the UCPD coherent with the AVMSD (and its interpretation by national authorities in their guidelines or enforcement	- Examples of scenarios where the applicable rules result in discrepancies, inconsistencies or complementarities, per law and per focus area. - Degree to which the identified discrepancies, inconsistencies or complementarities impact the coherence of the EU legal framework. - Degree to which the identified interfaces impact the coherence of the EU legal framework.	

Evaluation Questions	Sub-questions	Indicators	Data sources
	actions) regarding the regulation of influencer marketing? - To what extent are the CRD's rules on pre-contractual information coherent with other EU and national interventions that have similar objectives in the context of digital content and services? - To what extent is the UCTD coherent with other EU interventions (e.g. the GDPR, ePrivacy Directive, DSA, DCD and Data Act) as regards unfair contract terms and contracts that involve the use of personal data?		
EU Added Value			
13. What is the additional value resulting from the application of the Directives in the digital area?	- To what extent has the EU legal framework achieved positive impacts in the digital area and to what extent can these impacts be attributed to the three Directives? - To what extent were the identified positive impacts achieved at a reasonable cost, in a timely manner and without duplication across the legal framework? - In which areas has the EU added value of the Directives been less evident?	- Assessment of the effectiveness, efficiency and coherence of the Directives in the digital area. - Perceptions on how market practices will develop in future and their impact on the Directives. - Perceptions on how market practices would have developed in the digital area in the absence of the Directives and its impact on consumer protection.	- Desk research - Interview programme - Public consultation - Targeted survey - Consumer survey - Business survey - Case studies
14. In the absence of EU level action, to what extent could Member States have the ability or possibility to	- How would national level interventions to address problematic B2C practices in the digital environment have developed in the absence of EU provisions in the three Directives?	- Perceptions on how Member States could regulate problematic practices in the absence of explicit EU	

Evaluation Questions	Sub-questions	Indicators	Data sources
put in place appropriate measures to address the problematic practices in the digital environment?	- Given the level of harmonisation in the three Directives, to what extent could Member States have the ability to further regulate the problematic practices? - To what extent have requirements concerning issues such as influencer marketing and the termination of consumer contracts for digital services and subscription renewal developed, in the absence of explicit rules at EU level? How far would an EU level action help to establish a level playing field? - What impact would the reliance on Member State interventions alone impact the situation with regard to these issues across the EU?	provisions and their impact on consumer protection, taking into account the level of harmonisation in the Directives. - Perceptions of anticipated EU level legislative and non-legislative action to address challenges and perceptions on their impact.	

Annex IV. Overview of benefits and costs

Table. Overview of costs and benefits identified in the evaluation						
	Consumers		Businesses		Administrations (national competent authorities)	
	Quantitative	Comment	Quantitative	Comment	Quantitative	Comment
Costs description: The main costs of the existing regulatory framework are supported by traders who have to comply with the legal requirements in the digital environment. The total number of traders affected by consumer law compliance in the digital environment is 1.3 million. There are administrative costs from checking compliance and adjustment costs from having to redesign processes or websites to ensure compliance, but the consultations have suggested that these costs are not significant. There are no direct costs to consumers, but they experience detriment due to traders' non-compliance with the legal requirements and other problematic practices. The costs for administrations include the regular enforcement costs of implementing the legislation, such as complaint handling, inspection and monitoring costs, which are estimated to be higher for the digital environment, compared to offline. Overall, the costs associated with the application of the three Directives in the digital environment can be considered proportionate to the benefits. In the targeted survey, 51% of respondents found the costs to be well-balanced, while 24% considered the regulatory compliance costs to outweigh the benefits.						
Direct compliance costs: adjustment costs for businesses (one-off), notably concerning familiarisation with the law and initial compliance planning; and	N/a		Adjustment costs are estimated to range between EUR 208 – 303m per year.	In the business survey, only 10% reported incurring 'high costs' relating to adjustment and implementing legal requirements into business procedures. For compliant traders, these costs are largely one-off but they may include minor recurring costs to double check compliance, verify when	N/a	

adjusting business practices.			new design interfaces are launched, changes to T&Cs are published etc. 48% of business respondents noted that between 1-2 employees were responsible for the adjustment practices, with the majority dedicating between 11 and 20 days. Overall, 35% of traders could not provide a cost estimate, 49% provided a cost of EUR 2000 or lower, and 16% reported greater than EUR 2000 in costs.	
Direct compliance costs: administrative costs for businesses (recurring annually), notably checking compliance with	N/a	Administrative costs are estimated to range between EUR 249.8 – 487.5m per year.	In the business survey, only 15% reported incurring 'high costs' relating to administrative costs such as compliance checks. 67% reported checking at least once every six months that advertising/marketing and standard contract terms for online sales still comply with the law. 50% checked more	N/a

the law and information costs.			frequently, at least once every three months. For those experiencing costs, the dedicated resources in terms of employees and number of worked days were similar to those incurred for adjustment – 2 employees working for 21 days per year.		
Enforcement costs	N/a	N/a		No specific figures provided by CPAs, but moderately higher costs (25-30%) estimated for applying consumer law in the digital environment compared with offline.	CPAs considered enforcement actions in the digital environment to be more complex and costly due to various reasons (e.g. complexity and opacity of digital technologies, asymmetries during investigations requiring information disclosures from traders, legal cases covering application of consumer law in conjunction with data and digital laws). In terms of the additional costs associated with

						the changes introduced by MD, too early to assess since the provisions apply from 28 May 2022.
Benefits description: Consumers directly benefit from stronger protections and information disclosure, which is reflected in their increased uptake of e-commerce and digital services. Businesses benefit directly from a more level playing field across the EU and indirectly from the benefits of increased consumer trust, especially in the cross-border context. Authorities are able to engage in more effective cross-border enforcement cooperation thanks to a common framework of harmonised rules.						
Direct benefits: increased consumer protection; regulatory certainty and level playing field; cross-border enforcement cooperation.	-	Consumers benefit directly from increased protection, including several individual rights (e.g. 14-day right of withdrawal from online purchases, MD introduced a right to civil remedies in case of unfair practices), less exposure to unfair practices and unfair contract terms, as well as additional information disclosure that contributes to greater consumer choice and	-	In the business survey, a majority of traders recognised benefits as regards creating a level playing field across the EU for advertising and marketing (79%) and B2C contracts (75%), improving regulatory certainty for businesses (77%) and harmonising legislation to make it easier to sell cross-border (60%). In the targeted survey, 40% of stakeholders considered the existing laws to have a positive impact on the increase in e-commerce across the EU.	-	Authorities mainly benefit from the increased regulatory certainty about the applicable rules in areas that are harmonised at EU level. Harmonised rules also facilitate cross-border enforcement cooperation through common positions in the CPC Network and enable the exchange of best practices and information with other authorities. In case CPC sweeps uncover non-compliance by traders located in

		confidence in digital markets.		Concretely, 25% recognised an effect on increased cross-border trading, while 23% recognised it within their own Member State.		another Member State, those national authorities can directly benefit from the results of the investigation and take follow-up action.
Indirect benefits: increased consumer trust benefitting traders; increased deterrence reduces enforcement costs.	-	As a proxy for consumer trust, the 2023 CCS shows that the percentage of consumers conducting online transactions has increased from 57.8% in 2016 to 71% in 2022 and the consumer survey shows that 83% of consumers made some form of online purchase or used a product or service online in 2022-2023, which confirms that consumers are actively participating in digital markets. In the consumer survey, 6% of consumers indicated that they	-	In the business survey, a majority of traders also recognised indirect benefits as regards strengthened consumer trust in making purchases online (87%), ensuring fairness for consumers in the digital environment (80%) and striking the right balance between consumer protection whilst not overburdening traders (79%). Businesses benefit from increased consumer confidence, as shown by the high figures of consumers engaging in online transactions, both domestically and cross-border.	-	Authorities may benefit from the more deterrent fines and civil remedies introduced by the MD in the three Directives because they should reduce non-compliance in the future and thereby also reduce the costs necessary for enforcement.

		are ‘very trusting’ of online businesses, whereas 43% were ‘somewhat trusting’ and a further 37% ‘a little trusting’.				

Annex V. Stakeholders consultation - Synopsis report

Several consultation activities were carried out for this Fitness Check, including a call for evidence, public consultation, targeted consultations (consumer survey, business survey, targeted stakeholder survey, interviews), public events and meetings. A brief summary of the results of the consultations is presented below. More details can be found in the Annexes of the supporting study.

These consultation activities were highly valuable sources of a broad range of opinions, information and data that complemented the findings from desk research and literature review. The results have fed into the Fitness Check report - several references to the consultations, especially to the public consultation, targeted stakeholder survey, consumer survey and business survey, can be found in the main text of the Fitness Check report and in Annex VI on problematic practices.

Call for evidence[187]

The call for evidence was open between 17 May 2022 and 14 June 2022. 68 responses were received[188] from 14 Member States and the United Kingdom, followed by 3 delayed responses that were sent via email. Replies came from EU citizens[189] (39), business associations (13), companies (7), non-governmental organisations (4), consumer organisations (1), public authorities (4) and others (3), with the responses originating mostly from Slovakia, Germany and Belgium (26%, 24% and 21%, respectively). Four EU Member states' authorities provided a response: consumer protection authorities from Finland and the Netherlands, and ministries from Austria and Denmark. Responses were received from a broad spectrum of stakeholders, including national, EU and international consumer and industry organisations, individual companies, and from across sectors as diverse as airlines and food delivery services, and from online platforms.

In general, most respondents welcomed the Commission's decision to conduct a Fitness Check in this area. Regarding the general question of whether or not current rules are overall fit for digital environment, there are differences of opinion between consumer organisations and national authorities on one hand and business stakeholders on the other. Consumer organisations and authorities tend to see more legal gaps than business-oriented stakeholders. According to consumer organisations and authorities, the current framework needs to better keep up with technological developments, while business associations find the current rules provide sufficiently high level of consumer protection and repeatedly warn against new rules potentially stifling innovation and mostly advocate for technology-neutrality. There was agreement among several respondents about the importance of effective enforcement, examining coherence between EU consumer law and the recently adopted digital legislation, and the need to look further into specific unfair practices (e.g. dark patterns), taking into account behavioural insights.

Traders and business associations additionally highlighted that EU traders act in good faith and strive for improving the digital environment for consumers, and that a one-size-fits-all approach will fail to capture the complexity and differentiation of business models.

[187] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

[188] Feedback is publicly available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/feedback_en?p_id=30798773

[189] It is to be noted that there were several responses from anonymous citizens expressing resistance against more surveillance at EU level, which is not related to the scope of the Fitness Check.

Dialogue between stakeholders (especially with the Commission, industry, consumer associations and regulatory authorities) was found to be key to better awareness, application and enforcement of rules. Enforcement authorities have strong powers but need to be provided with sufficient resources and skills to act effectively in their investigations. Transparency requirements should be balanced between all parties in the chain of commerce, and not just imposed on retailers. Personalisation practices should not be viewed as unfair *per se*. In general, they called for clearly mapping any remaining legal gaps and to distinguish those from areas where enforcement is lacking.

Consumer organisations and other NGOs additionally highlighted that many consumers can be vulnerable in the digital environment. New technologies make it possible for traders to strengthen their position over the consumer, which can distort the consumer's autonomous decision-making. Under conditions of digital asymmetry, the burden of proof could be shifted more towards the trader. Key concerns were raised regarding specific practices exploiting consumer vulnerabilities, such as those that trigger addictive responses in consumers (related to and within this issue: gamification, loot boxes, in-game and in-app currencies, NFT and possibly wider blockchain transactions), retain and exploit the consumer's attention, feeding off their personal data and time as currency (infinity scroll, auto-play, notifications), take advantage of consumers' dynamic inconsistent preferences and can result in significant consumer harm without necessarily being misleading or aggressive (algorithmic profiling, automated decision-making, and predictive analysis) and contract terms preventing consumers from exercising their rights under copyright law (e.g. format shifting, sharing content within family, or private copies; and terms which oblige the consumer to conclude an additional digital content contract or a contract pertaining to hardware with a third party). They often considered that the UCPD blacklist should be updated and provide clearer definitions, while also taking into account that the rapidly changing nature of digital technologies may make the enforcement and identification of such practices quickly outdated. They also flagged the need to examine the use of virtual assistants, including voice shopping.

National authorities additionally highlighted the need for a holistic and principle-led approach together with specific blacklists for legal certainty. On the business' side, they noted that there is an insufficient focus on the ethical and legal limitations of the use of persuasive techniques. There was support for omni-channel neutrality but also the need to anticipate in legislation the effects of more immersive digital spaces on consumer choices, and an awareness of the differences across platforms and digital ecosystems. Consumer protection should be embedded by design, with greater responsibility with the digital service providers in making sure that the design of these platforms, functions and the products provided on the platforms are not to the detriment of vulnerable consumers. Caution is needed when adding new information disclosure requirements, as they are not always effective, and the simplification of information provision to consumers should be further explored. They also highlighted the need to make it compulsory for traders to provide information of the total cost of a subscription contract and further information on the nature of a continuing obligation. They flagged the need to enhance the protection of children, in alignment with the BIK+ strategy's focus on creating more age-appropriate digital services, and to further regulate loot boxes and to consider further regulating addictive design features such as snap streaks, autoplay and infinite scrolling. Overall, they stressed the need for more resources for enforcement and greater cooperation and exchange of research among authorities.

Public consultation[190]

The public consultation ran between 28 November 2022 and 20 February 2023. The questionnaire addressed perceptions as to how prevalent problematic practices are in the digital environment, what actions consumers took to resolve problems, perceptions of the current level of consumer protection in the digital environment and possible solutions to the identified problems. First part named "consumer questionnaire" was addressed to citizens (consumers), and only respondents selecting EU or non-EU citizen in a question at the beginning of the questionnaire were directed to this part. Second part ("In-depth questionnaire) targeted stakeholders involved in the implementation of the directives (all stakeholder types other than EU citizen or non-EU citizen started directly in that second part). Both parts included closed questions as well as open-ended questions with free text option. The consultation was available in all 24 official EU-languages.

350 online responses were received through the website, followed by 19 delayed responses that were sent via email. The graphs/statistical overviews of answers to survey questions reflect the 350 responses submitted through the website, while the delayed responses were still taken into account in the overall analysis. The responses included 71 position papers. Website responses came from EU citizens (61%, 214), followed by business associations (15.7%, 55), companies 7.4% (26), NGO's (4%, 14), public authorities (3.4%, 12), consumer organisations (2.9%, 10), non-EU citizens (2.3%, 8), academic/research institutions (0.9%, 3), trade unions (0.3%, 1) and others (2.0%, 7). Most responses came from EU countries, notably from Portugal, Belgium, Germany, Italy and Spain. 95% (332) of responses came from within the EU and 5% (18) from non-EU countries. Out of 128 respondents who answered the question on the organisation size, 27% (34) responded that they are large (250 or more employees), 17% (22) medium (50 to 249 employees), 24% (31) small (10 to 49 employees) and 32% (41) micro (1 to 9 employees).

The consumer questionnaire section of the public consultation showed that the problematic practice mentioned as occurring most frequently[191] was the requirement to share payment/credit card information to access a free trial for a digital service, 91% of the 222 citizens faced this issue, including 64% (141 out of 222) experiencing it three times a year or more. 89% mentioned they found website or app designs confusing or deceptive, suggesting that despite being subject to different provisions in EU consumer law, dark patterns remain a problem. 74% experienced a lack of disclosure regarding paid promotions by social media influencers. 74% reported that they were victims of data misuse for personalised commercial offers, e.g. by showing content which potentially utilised information about a consumer's weaknesses or vulnerabilities. Subscriptions were sometimes viewed as being difficult to cancel (69%) and consumers were automatically charged for a subscription without receiving any reminder about the renewal (62%). 34% indicated experiencing the issue of cancelling subscriptions being only possible after a longer subscription time while paying monthly. Consumers also felt that they had been faced with unfair terms when buying a digital service or content but had nevertheless agreed (63%). 33% reported spending too much time or money using certain websites and apps for hours (e.g. due to incentives or rewards for spending more time), while 57% of

[190] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/public-consultation_en

[191] In the past 12 months, have you experienced any of the following problems online, and if yes, what frequency? (n=222)

consumers reported having never faced an issue.[192] 47% reported experiencing a lack of clarity about the price of in-app purchases, at least once in the past year.

22% (48 out of 222) of consumers stated that they have sufficient knowledge of EU consumer rights in the digital environment, 55% felt they had some knowledge, and 23% felt they didn't have enough knowledge. When asked to reflect about the most serious problem they encountered in the past year and how they solved it, 88% (193 of 220) of consumers did not take action to solve the problems they encountered, only 12% (27) said they did. Out of 27, 19 (70%) complained to the service provider, such as a website or app developer. Eight[193] complained to consumer protection authorities (30%), two (7%) to a consumer association, one (4%) complained to a European Consumer Centre (ECC) and one (4%) complained to an ADR. Only 20% (44 out of 220) were able to solve the problem fully, 8% to a large extent and 15% to some extent. 45% stated that they were not able to solve the problem at all.

The second questionnaire of the public consultation was targeting stakeholders but remained open also to consumers that replied to the first section: 58% (129) answered first part only, and 42% (93) answered both Parts 1 and 2 in addition to all other types of stakeholders (127) that were led directly to the second part. The responses[194] showed the following:

- 92% of 221 respondents agreed that a strong legal framework is required to protect consumer interest in the digital environment.
- 82% agreed that there needs to be uniform legislation across the EU.
- There is some scope for simplification and burden reduction in existing EU consumer laws (64%), supported further in the stakeholder position papers by both trader and consumer representatives.
- The existing legal framework sufficiently protects consumers in the digital enviroment (48%).
- There are some legal gaps and/or uncertainties in the current EU consumer law framework (52%).
- Traders comply well with existing EU consumer law in the digital environment (42%), (25% disagreed with this).
- 27% disagreed and 32% agreed that existing EU consumer laws are coherent with other EU legislation in the digital area (e.g. data protection, regulations applicable to online platforms, artificial intelligence).

Stakeholders were also asked[195] to evaluate the impact of EU consumer law on selected areas in the digital environment. The percentages represent those indicating positive impact (aggregated "rather positive" and "very positive"):

- Protecting consumers against unfair commercial practices (71%).
- The protection of vulnerable consumers (53%).
- A level playing field among businesses addressing the needs of consumers (49%).
- Amount and relevance of information provision to consumers (54%).
- Enforcement regarding cross-border infringements through the CPC network (42%).

[192] It is argued and understood in the wider literature that digital addiction, like many other addictions, may be neither realised nor accepted by the individual in some cases.
[193] Some respondents selected more than one answer option as they had taken different type of actions, therefore there is some overlap between the numbers, and the total of the selected answers is more than 27 (i.e. 32).
[194] To what extent do you agree or disagree with the following statements? (n=221)
[195] How positive / negative has the impact of the existing EU consumer law framework been on the following aspects in the digital environment? (n=221)

- Increasing cross-border e-commerce (42%).
- The competitiveness of EU vs. non-EU businesses (28%). 25% were neutral, 26% were negative.
- Increase of national e-commerce, 34% in total were positive. 29% neutral, 14% negative.
- Prices of products (27%). 24% negative. 30% neutral.
- Number of customers and revenues for businesses supplying consumers in the EU (25%). 30% neutral, 17% negative.

Stakeholders were then asked about how strongly they agree or disagree with potential suggestions to improve EU consumer law (n=221). An overview of the responses – ordered from strongest support through to most moderate support - is provided:

- 70% supported a requirement of receiving an email confirmation when a contract has been terminated;
- 67% supported requiring express consent when switching from a free trial to a subscription service;
- 65% supported the statement that where automation bots are used to deal with consumer complaints and other inquiries, consumers should have the possibility of contacting a human interlocuter upon request.
- 63% supported further regulating dark patterns;
- 63% supported providing consumers a summary of T&Cs;
- 63% supported sending a reminder about a subscription automatically renewing;
- 63% agreed that there is a need for stronger protection against digital practices that unfairly influence consumer decision-making (e.g. manipulative website design or misleading presentation of yes/ no answers);
- 63% supported technical means to make cancellations easier (e.g. using buttons);
- 60% supported limiting the possibility of automated buying using bots of popular products in order to resell at higher prices;
- 60% supported the statement that 'signing up for a free trial should not require any payment details from consumers';
- 59% supported reminders about subscriptions after a period of inactivity;
- 58% agreed that clarifying the concept of an influencer and the obligations of such traders towards consumers would be beneficial;
- 53% agreed with the statement that more specific information obligations should apply when products such as event tickets are sold in secondary markets.;
- 53% agreed with the statement that the concept of the trader's professional diligence towards consumers should be further clarified in the digital context;
- 53% supported more price transparency when buying virtual games with intermediate virtual currency;
- 53% supported the idea of shifting the burden of proof of compliance with legal requirements to the trader in certain circumstances;
- 51% agreed that the concept of the average consumer or vulnerable consumer could be adapted or complemented by other digital benchmarks;
- 51% supported the need for more transparency regarding the possibility of obtaining specific items from paid content that has a randomisation element (e.g. paid lootboxes);
- 47% supported the possibility of having an explicit option to receive non-personalised offers (while only 26% disagreed);

For certain more technical topics, namely the suggestions of allowing consumers to set limits to the amount of time and money spent using digital services and mandating more

price transparency when buying virtual items with intermediate currency, although majority of respondents supported these ideas, there was a relatively high percentage of "don't know" responses, as high as 25% in the case of virtual items and currencies.

In addition to the responses to the questionnaire, there were 71 position papers received from national and EU-level consumer and business associations, large multinational firms including online marketplaces and platforms[196]. In addition, a wide range of other sectors were represented, such as e-commerce retailers, software, computer and telecoms companies, the gaming industry, travel industry, the restaurant and hotel industry, food industry, film distributors.

Overall, many traders and business associations considered that the current EU consumer law framework offers broadly adequate consumer protection in the digital environment. However, according to many stakeholders applying the laws (especially consumer organisations, ministries and consumer protection authorities) EU consumer law could be strengthened to tackle specific problematic practices. Some stakeholders requested greater clarity as to the overarching concept of 'digital fairness'. The main views expressed are similar to those expressed in other consultations, with consumer associations seeing more legal gaps and issues, and business stakeholders in particular in the digital world advocating for principle-based legislation and many stakeholders stressing the importance of first focusing on implementation and enforcement of current rules. National authorities were favourable to the idea of alleviating the burden of proof in areas where there is a significant digital asymmetry to the detriment of the consumer. They also highlighted that they will have to adapt their tools of investigation and identification of violations through a machine-based approach, such as web crawling.

According to major online marketplaces and national authorities, the DSA provides an appropriate level of protection against aggressive practices including dark patterns, some pointing also to the MD as covering the issues. However, there remain calls for broader recognition of specific types of dark patterns, noting that not all practices which influence consumer decision making fall under the current category of unfair commercial practice, and that the blacklist of aggressive commercial practices in Annex I of the UCPD must be added as a complement to the general clauses of the legislation.

The topic of consumer vulnerability, and specifically among consumer associations, the issue of what defines an 'average consumer', is a prominent topic raised. Trade organisations typically agree that the current legislative framework already addresses consumer vulnerability, both through prohibitions on misleading practices and through the right to withdraw from contractual agreements under the CRD. Nonetheless, most stakeholders agree regarding the need for ongoing efforts to protect minors in the online environment. According to several industry associations and traders, the definitions of professional diligence, average consumer, and vulnerable consumer do not require any modification. A large platform contends that achieving a higher level of consumer protection based on individual characteristics and personal circumstances can be done more effectively through consumer education and information campaigns.

Overall, there is an acknowledgement across stakeholders that digital addiction (including in connection with loot boxes) pose a threat to the most vulnerable consumers and that there is a need for more transparency regarding the probability of obtaining specific items from paid content that has a randomisation element (e.g. prize wheels, loot/mystery boxes in video games, card packs). Suggestions in line with this include the disabling of in-game

[196] Significant actors across the digital economy in terms of both market share and industry innovation submitted position papers, such as Amazon, Google, Meta and Apple.

payments and loot boxes by default, and that consumers should have the option to use the game without algorithmically driven decision-making that aims to influence consumer behaviour. With respect to minors playing online games, consumer organisations suggest that a ban should be introduced on offering loot boxes, 'pay-to-win' mechanisms or other randomised content in exchange for real money in games that are likely to be accessed by minors.

The position papers portray a full spectrum of views relating to online subscriptions and potential amendments to current EU legislation in this regard. In general, stakeholders agree that greater accessibility to online subscription information could be highly beneficial in addressing knowledge imbalances. Moreover, many also agree that a simple cancellation process would be of benefit to the consumer. Consumer organisations and national authorities tend to be in favour of introducing further regulations and policies which shift the burden of responsibility towards traders, whilst trade organisations are more sceptical of such changes. On the topic of free trial periods and the automatic renewal/conversion to a paid subscription, several stakeholders argue that a free trial should not require any payment details from consumers; and that express consent should be required when switching from a free trial to a paid service; and that traders should be obliged to send reminders to consumers before automatic subscription renewals occur. A large online platform however expressed concern that the introduction of notifications and requests for further consent may risk confusing, panicking or irritating the consumer.

On the other hand, online traders and organisations tend to agree that the current provisions successfully protect consumers who benefit from online subscriptions. However, they state that requesting payment information from consumers during free trials is a necessary element of their business model, and that the implementation of further regulations in this regard may disrupt their business practices.

Whilst trade organisations highlight the consumer benefits of personalisation practices, consumer associations and authorities argue that giving (or removing) consent for personalised offers, products and advertising allows for greater consumer choice. National authorities recognised the benefits of personalisation, provided it does not exploit, discriminate, or exclude consumers. Most trade organisations, online and e-commerce platforms believe that current EU consumer law successfully regulates personalisation practices relating to advertising and promotions by keeping a general principles-based approach. In addition to this, some point to the DSA as a newly introduced, and not yet fully implemented but crucial piece of legislation, offering vital protection against misleading advertising and exploitation of vulnerabilities. For some traders and marketplace platform service providers, the ability to rely on targeted – or personalised – advertising is reported as absolutely essential.

Overall opinions regarding social media influencers were divided threefold: consumer-oriented organisations and few other stakeholders advocated for a better definition of the concept, more transparency and some for prohibitions of marketing certain products/services (including to prevent regulatory fragmentation through national legislation). Trader-oriented organisations argued that influencers are already extensively *de facto* regulated in current EU consumer law, even if there is no definition of an influencer as a specific category of trader. Finally, a few entities requested further transparency requirements for influencers when they are engaging in paid promotions. Many stakeholders, including authorities, argue that the current situation is one of high legal uncertainty, and legislative action to clarify this concept would in their view be highly advisable. Consumer organisations consider that the promotion of illegal products and services by influencers should constitute an unfair commercial practice and be blacklisted

in the UCPD. A digital organisation moreover notes that the DSA and AVMSD also introduce helpful transparency standards on user-generated commercial content. Moreover, they consider that consumers are increasingly savvy to the world of influencer marketing and sales of products and understand the commercial nature of such communications.

Targeted survey

The targeted stakeholder survey was conducted by an external contractor for the supporting study using an online survey tool. Out of 164 respondents, there were 66 business associations (40%), 17 traders (10%), 19 consumer associations/NGOs (12%), 10 ECCs (6%), 10 national ministries (6%), 20 national enforcement authorities (12%), 22 academic researchers and others (13%). 12 of the 17 traders were large firms of 250 or more staff (71%), with many SMEs represented as members of business associations. 26% of respondents were EU-level associations, from Germany (15%), Belgium (10%) and Austria (6%). There was representation from at least one individual respondent across the majority of Member States (24/27), excluding Estonia, Luxembourg and Greece. 65% of responding enterprises (traders at large and SMEs speaking independently and represented by associations) engage in trade on a cross-border basis within the EU and internationally. Only 12% of respondents operate cross-border but solely within the EU.

Stakeholders were asked about the impact of EU consumer law on several aspects. The most prominent contribution of the Directives was perceived to be the facilitation of e-commerce trough uniform rules on the right to cancel online purchases within 14 days (47% to a great extent). Stakeholder uncertainty was greatest with regard to ensuring transparency and fairness in the marketing of virtual items (42% don't know, 11% not at all). Overall, the most positively perceived impact of the EU consumer law directives is on strengthening consumer protection and trust, facilitating e-commerce through uniform rules on both unfair commercial practices and distance contracts and the overall functioning of the EU digital single market.

33% of respondents see outstanding legal gaps, while 42% did not perceive such gaps and the rest did not know.[197] Between 27% and 63% of respondents considered that the Directives provided legal certainty in many specific areas to a great or moderate extent.[198] It is to be noted that across all areas the share of "don't know" answers is significant: between 22% and 53%. Areas with the highest share(s) of respondents selecting great or moderate extent:

- online sale of digital content and services (22% to great extent, 39% to moderate extent)
- online sale of physical products and services (29% and 34%)
- standard contract terms (23% and 34%)
- rules on burden of proof in disputes/ enforcement of fairness requirements (20% and 30%)

When respondents were asked which of the listed practices were problematic, the share of 'don't know' responses were quite high (27%-63%) across the long list.[199] The practices selected as "problematic" by most respondents are (combined 'strongly agree' and 'agree'):

[197] Q14 Do you perceive that there are any outstanding legal gaps? N=163
[198] Q13: To what extent have the EU consumer law directives provided regulatory certainty about the applicable rules in the following specific areas (n=163)
[199] Q16 To what extent do you agree or disagree that the following practices are problematic (N=144). Answer options were 'strongly agree, agree, disagree, strongly disagree and don't know'.

- Lack of transparency concerning paid promotions in social media (57%)
- Deceptive practices (dark patterns) in website/app design (54%)
- Use of consumer data that exploits specific vulnerabilities for commercial purposes (46%)
- Lack of clear and intelligible presentation of contractual information (45%)
- Problems due to automatic conversion of free trials into paid subscriptions (42%)

Respondents perceive potentially problematic B2C digital practices as increasing rather than decreasing, with the highest scoring practices being (percentages are combined 'increase' and 'significant increase'):

- Loot boxes and addictive design (69% indicating increase)
- Scalping of products using automated software (except event tickets) (68% indicating an increase)
- AI systems deploying subliminal techniques beyond a person's consciousness for commercial purposes (68% indicating an increase).[200]

45% of respondents strongly agree that it is proportionate to keep the burden of proof on consumers to provide evidence of an infringement. However, the opinions on the two alternatives implying some degree of reversal of that burden, appear to be quite divided: 31% strongly agree that the burden of proof should be put on traders to demonstrate fairness in cases of major digital asymmetries, 36% strongly disagree (the scores of combined agree-strongly agree and disagree-strongly disagree are very similar, 46% and 48% respectively). 25% strongly agree that the burden of proof should be shifted in certain circumstances (e.g. if there is reasonable suspicion of an infringement), while 33% strongly disagree with this idea (combined scores are again even closer: 45% agree-strongly agree and 49% disagree-strongly disagree).[201]

According to respondents, the EU consumer law framework has generally provided significantly better outcomes than national level regulation could alone in all cases of addressing problematic practices and ensuring ease of trade and consumer redress across the single market. The areas of facilitating cross-border e-commerce, addressing problematic cross-border commercial practices, effective functioning of the digital single market through harmonized rules/avoidance of fragmentation were the areas where EU-added value was most valued with respectively 97%, 95% and 98% of respondents claiming them to record significant or moderate better outcomes.[202]

Most respondents agree that the EU consumer law framework and its application should be strengthened to address existing and/or anticipated future challenges in the area of enforcement. 75% supported more soft enforcement and more harmonised enforcement across the EU.[203]

From a list of potential legislative changes, the following gained highest support: requirement to indicate the real price of virtual items in digital products (62%), additional transparency about the dropshipping business model (i.e. the fact that the shop does not

[200] Q17: In the past five years, how far have the following potentially problematic B2C digital practices increased or decreased in frequency? N=90: significant increase, increase, no change, decrease and significant decrease.
[201] Q69 To what extent do you agree or disagree with the following statements [regarding burden of proof]? n=104, with answer options to each statement being: strongly agree, agree, neither agree nor disagree, disagree, strongly disagree.
[202] Q77: To what extent has the EU consumer law framework achieved better outcomes than could have been achieved by Member States regulating these areas themselves? N=95, answer options: significantly better through EU action, moderately better through EU action, significantly better through Member State action, moderately better through Member State action.
[203] Q80: How far do you agree that the EU consumer law framework and its application should be strengthened to address existing and/or anticipated future challenges in the area of enforcement?

hold those products in stock) (57%), specific rules to mitigate the negative effects on consumers of addiction inducing commercial practices in digital products and services (56%), and the prohibition to use contractual, technical or behavioural measures to bypass consumer law obligations (55%).[204]

In addition to the responses to the questionnaire, there were 16 position papers received. In many aspects, the papers echo those submitted to the call for evidence and public consultation. Many traders (both online and offline focused) repeated prior calls to respect principles of technology and channel neutrality, and a need for further enforcement and implementation of existing legislation. Caution has also been called for regarding the presentation of potentially problematic practices (e.g. personalisation) which have been shown to have many benefits for consumers. Individual traders, trade associations and platforms praise the flexibility and future-proofness of current rules. However, for this effectiveness to continue and to be further enhanced, technical understanding by judges must be sufficiently high. This could require traders and authorities to coordinate to facilitate knowledge transfer and greater transparency around new technological practices and innovative business models.

Traders and platforms argued that the concept of dark patterns is rather "a new branding of a well-known activity, which refers to deceptive commercial practices – covered by UCPD, complemented by DSA", and cautioned that new definitions may lead to more uncertainty. However, according to a national authority, the cumulative effects of dark patterns on consumers should be still considered, especially in vulnerable categories, and with the interplay with targeted personalised offers and content, requires a concerted approach between actors across policy fields.

An authority advocates for a shift in the burden of proof to actors in the digital goods and services supply chain, by creating legal liability for third-party facilitators. Some traders are wary of potential additional regulatory burdens and information requirements, and subsequent liability risks, especially for SMEs. An authority suggests to re-evaluate existing transparency requirements for effectiveness and usefulness and to encourage businesses to inform themselves about the effects of their own current digital commercial techniques.

Some digital stakeholders question the need for a subscription cancellation button in view of the DCD, which already includes detailed provisions on contract termination. There were also calls to consider greater nuance in the information requirements regarding the trader's geographical address in cases where it is both their professional and personal home address. As an alternative approach, it was suggested that it would be sufficient to require the publication of a registered business ID number, an email address, phone number and a country of establishment, so that consumers and enforcement authorities can nonetheless access geographic addresses through local business registers.

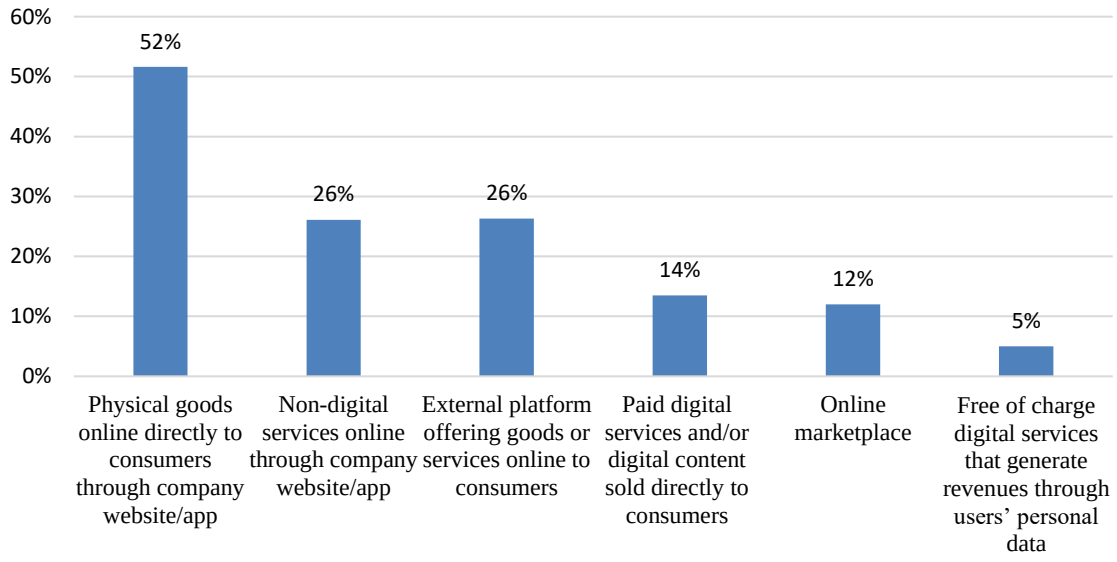
Different stakeholders agreed that in-game purchases and games of chance are now more often forming a key component of the overall game experience. While loot boxes are no longer a new phenomenon, their prevalence in combination with the rise of online promotional activities, such as the pervasive promotion of gambling and betting websites by influencers, present a significant challenge. More transparency requirements are suggested on the probability of obtaining specific items from paid content with randomised elements and concerning the display of prices in real currencies.

[204] Q82: What are your views on specific possible changes to the existing EU legal framework which could be considered to strengthen consumer protection and to address problematic practices and/ or legal gaps? (n=98). Share of combined 'agree + strongly agree' ranged from 41% to 62% with 10-20% 'neutral' answers to each potential change.

Business survey

The business survey was conducted by an external contractor for the supporting study, with a sample of 1000 companies of various sizes, sectors and business focus from a selection of 10 Member States[205]. 34% were from the retail sector, more concretely retail sale of computers, peripheral units and software (17%), information and communication equipment (6%), retail sale of telecommunications equipment (6%) and retail sale of audio and video equipment (5%). Other sectors included gas and electricity services (25%), telecommunications (14%), manufacture of computer, electronic and optical products (14%) and manufacture of electrical equipment (12%). 55% have 9 employees or fewer ('small businesses'). 52% indicated selling physical goods online directly to consumers through their company website or app. 26% indicated selling non-digital services online (e.g. accommodation).

Figure 13 - Types of products or services provided by the traders responding to the business survey (n=1000)



- According to 66% of businesses, current legal obligations to their company are clear, according to 32% they are somewhat clear.[206]
- 64% indicated the sale of online goods as an area that led to legal uncertainty. This was higher for smaller companies (76% for companies of 1-5 people), than for larger companies (44% in companies of 55-250 employees).[207]
- Overall, 92% of respondents found the legislation was either very well adapted (16%) or well adapted (76%) to new technological developments. Companies of 50-250 employees were the least positive with 21% indicating legislation was poorly adapted.
- 87% indicated they had taken specific measures to ensure that their online interface is user-friendly and transparent. Of these 869, 44% indicated that 1-2 employees worked on these measures. Overall, companies dedicated an average of 3.1 employees to the measures. 64% of companies with 250+ employees indicated having dedicated 5 or more employees. 47% of companies dedicated between 11 and 20 days.[208]

[205] France, Germany, Italy, Spain, Sweden, Portugal, Poland, Romania, Hungary, Estonia.
[206] Q7 Are the current legal obligations from the EU and national consumer legislation applicable to your company clear?
[207] Q8 In your opinion, do any of the following involve legal uncertainty for your company? Please select all that apply.
[208] Q10 Have you ever taken any specific measures to ensure that the online interface (meaning the design of your website or app) is fair, user-friendly and transparent? Q.10.1 Please estimate the initial resources you invested to implement the measures. Q.10.2 Please estimate the recurring annual costs related to these measures.

- 76% indicated they had not collected personal data from customers. Larger and medium sized companies were more likely to have gathered personal data from companies, with the highest portion from companies of 10-49 employees (32%).[209]
- Of the 236 that indicated having collected data, most used the data to help decide which offers to feature more prominently (31%) or decide how to tailor/customise advertisements shown to customers (30%).[210]
- In the past 12 months, 20% of companies, mostly retailers, had offered subscriptions to consumers for any type of product or service offered online.[211]
- 87% indicated having not refused to cancel subscriptions after a customer requested it. Of those that had refused, 48% did so because the contract terms specified that the contract can be cancelled only at the end of the contractual period or after a certain time has passed.[212]
- Around 50%[213] indicated 'low costs' due to compliance with consumer law in the digital environment in each of the identified areas. *Familiarisation with rules, obligations and initial compliance planning* was the issue for which the largest share of respondents indicated high costs. *Information obligations* recorded the greatest percentage of 'no costs'.[214]
- 67% of respondents checked at least once every six months that advertising/marketing and standard contract terms for online sales are still complying with national legislation. More specifically, 50% checked at least once every three months.[215]
- Of those that sold products or services online to consumers in other EU countries,[216] the greatest percentage (46%) experienced no additional cost associated with entering a new market, 17% experienced high costs. The greatest percentage (28%) of those paying high costs were large companies (over 250 employees), though 53% of large companies experienced no costs and 19% low costs. Most companies indicated no costs in response to any compliance issues.[217]
- Most businesses noted a positive impact of harmonisation of rules on advertising/marketing and standard contract terms on each of the listed categories. [218] The highest positive impact was reported for *Strengthened trust among consumers in making purchases online* (87%). The area in which the largest amount of respondents indicated a negative impact was *Striking the right balance between consumer protection, whilst not overburdening traders,* though still low at 11%.

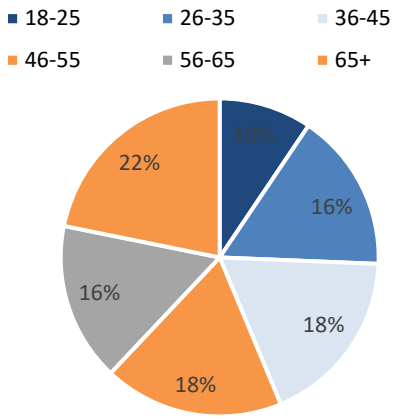
Consumer survey

[209] Q11 In the past 12 months, have you gathered personal data from customers that have visited your website?
[210] Q11.1. In the past 12 months, have you used customers' personal data to tailor/customise/optimise the appearance of your website, or the content displayed on your website?
[211] Q12 In the past 12 months, has your company offered subscriptions to consumers for any type of product or service offered online (e.g. via an app or website), including digital content and digital products or digital services (software, apps, e-books, online)
[212] Q13. In the past 12 months, has your company refused to cancel subscription contracts after a customer requested it?
[213] Between 47%-52% across four areas (see next footnote for the areas).
[214] Q14 To what extent has compliance with consumer law requirements resulted in the following types of costs for your business in the digital area?
[215] Q15. In recent years, how frequently have you checked that your advertising/marketing and standard contract terms for online sales still comply with national legislation?
[216] Only 13% indicated that in the last 12 months they had sold products or services online to consumers in other EU countries. (Q16. In the past 12 months have you been selling or providing your products or services online to consumers in other EU countries?)
[217] Q16.1. When you first entered the market in another EU country, did you face any additional costs to check compliance with and adjust your business practices to the legal requirements of that country, for example rules regarding advertising/marketing, cancellation of contracts and standard contract terms? This may include costs for legal advice, costs for adapting standard contract terms etc.
[218] Q18 Please indicate if the harmonisation of rules concerning advertising/marketing and standard contract terms for online sales has had a positive or negative impact on your company.

The consumer survey was conducted by an external contractor for the supporting study, with a sample of 10,000 respondents in the same 10 Member States as for the business survey. Consumers were first asked a series of questions to determine their key socio-demographic characteristics[219] as well as a number of profiling questions regarding their preferences.[220] Additional information about the distribution of age, gender and household total net income is provided in the graphs below.

Figure 14 - Age and gender distribution in the consumer survey (n=10000)

Age groups distribution



Gender distribution

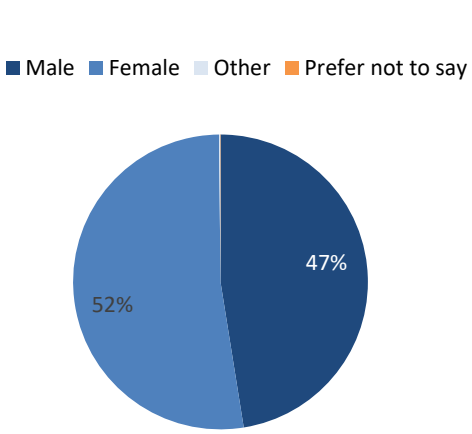
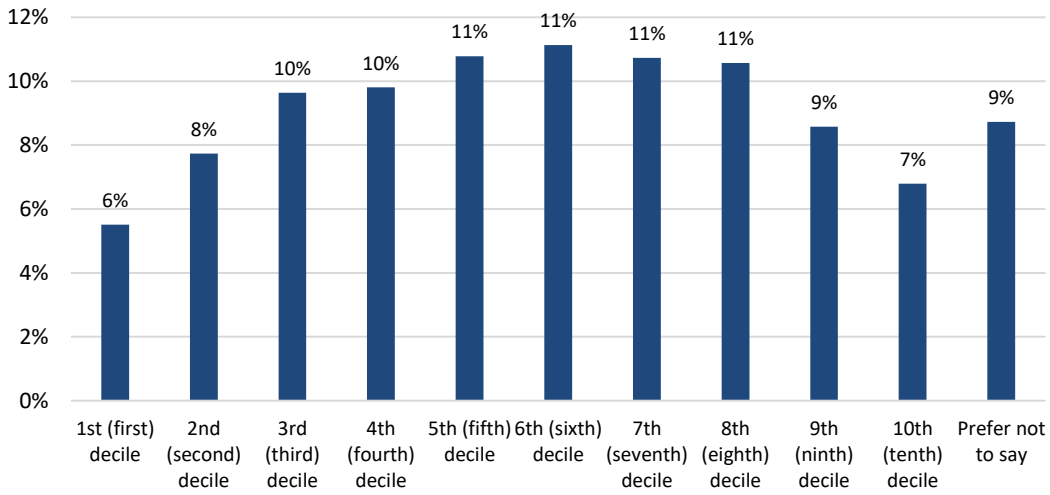


Figure 15 - Household total net income – Deciles distribution in the consumer survey (n=10000)



In the summary below, percentages often refer to the whole sample, while in specific questions to a sub-sample (e.g. to those who replied in a certain way in a previous question). For most answers below, the sums of the responses 'always', 'most of the time'

[219] Sample was gender-balanced, covered adults, with a balanced distribution across all age sub-groups from 18 to over 65-year-olds as well as across different income levels. More information on the sample as well as more detailed presentation of the results can be found in the support study.

[220] E.g. 83% had made some form of online purchase or used a product or service online in the past 12 months.

and ‘sometimes’ are combined. If a different combination was used, this is indicated in the sentence or footnote.

Consumers indicated among others the following:

- 54% had easily found a company phone number or email address, when purchasing online. 37% could not find or only found with difficulty this information.
- 56% indicated that when looking at customer reviews on websites, they could not find information about how the reviews are collected and whether the company ensures that published reviews are made by real customers.
- 66% indicated that while making purchases online, they had noticed a product they were looking at was low in stock or in high demand.
- 66% indicated that they had encountered conditional offers for purchasing multiple items and for purchases above a certain amount. 58% indicated they had experienced a presentation of a lower price for members of a loyalty programme.
- 64% of respondents indicated that in the preceding 12 months, they had used or purchased digital content/services/subscriptions. These respondents indicated mostly the following experiences:
  - 41% have realised post-purchase that additional fees were required to access certain features and that they had not been informed of this pre-purchase.
  - 35% have experienced challenges when making in-app purchases because prices were displayed in the app's virtual currency.
  - 48% have experienced a website or an app repeatedly asking them to make a decision online.
  - 35% have experienced that a content they were viewing (e.g. on social media) seemed to be a paid promotion or advertisement, but the website or app did not make this clear.
- 46% indicated they had experienced issues relating to the right of withdrawal.[221] 74% indicated they found it difficult to communicate with the seller about the missing reimbursement after withdrawal. 74% indicated experiencing difficulty when notifying the trader that they wish to withdraw. 72% reported not receiving clear information regarding whether they had the right to withdraw or if an exception applied. 73% also indicated that the design or language used on the website made it difficult to understand that they had the right to withdraw within 14 days.[222]
- 51% indicated that they had purchased, used, renewed, or cancelled a digital subscription in the preceding 12 months.
- 33% indicated they had activated a free trial user account in the preceding 12 months, out of these:
  - 71% indicated having provided personal payment information for a free trial, with only 10% indicating they were never asked for their payment information.
  - 50% experienced automatic extension of their accounts into a paid subscription, without them being aware this would happen. 24% indicated this ‘never’ happens.
  - 54% indicated cancelling the subscription at the end of the free trial was always or mostly easy, while for 40% it was sometimes, rarely or never easy.
- Regarding personal data, the most common experience indicated by 41% was that the design or language of the website/app made it difficult to understand how the consumer's personal data would be used.

[221] N=2745, consumers who encountered problems with exercising the right of withdrawal from online purchases.
[222] N=1250, problems experienced by consumers regarding the right of withdrawal.

- 38%[223] of consumers indicated that they have had difficulty understanding what kind of profile a platform created for them based on personal data and how this might affect the content presented to them.
- 59%[224] indicated that they read the Terms & Conditions at least some of the time.
- When specifically asked about the terms in their online contracts, respondents most commonly experienced two scenarios: the contract allowed the trader to keep and process their personal data even after the end of the contract (18%); and under the contract, the mere access to the site implied consent to the Terms & Conditions, even if they were not able to have access to them yet (17%).
- 27% of consumers (approximately 1 in 3 consumers surveyed) indicated they have experienced situations that have caused them financial loss, time loss or emotional distress. Of those who had experienced financial loss, time loss or emotional distress, when questioned about what product or service was involved in their most negative experience, 58% indicated the experience occurred when purchasing physical goods online, while one-third of the sample (33%) indicated it was an issue with digital content or services.
- Focusing on physical goods, when consumers who had experienced an issue were asked how they attempted to resolve it, the most common actions mentioned were making a complaint to the seller or provider (39%); and cancelling the purchase of the physical good or service within the cooling-off period (37%). 20% of consumers indicated that they chose to repair the product themselves, while a further 20% chose to replace the item at their own expense.
- According to respondents who attempted to resolve the issue, 20% of sellers/providers involved chose to refund the money, after the cancellation of the contract. Other reactions were: they acknowledged the problem (13%); they gave me an unsatisfactory explanation (12%); and they did not do anything (11%).
- 61%[225] of those who had attempted this process found they experienced difficulties or failed to solve a problem with the trader because it was difficult to supply the required evidence.
- As a result of their experiences making purchases online, 78%[226] mentioned distress.
- 61%[227] have knowledge about consumer rights that apply in the digital environment. 91% felt consumer rights are important for decisions related to the purchase or use of a product or service online. 61% have not been able to use EU or national consumer legislation to ensure respect for their rights.
- 60% felt consumer rights have not kept up with technological developments. 22% indicated that consumer rights are fully ensured.

Interviews

The interview programme was conducted by the external contractor for the supporting study to gather feedback on key evaluation issues across the different range of research topics, to complement and validate desk research findings, to provide input to case studies etc. In total, 101 interviews were conducted. The interviews were conducted based on a common set of questions for each stakeholder group, broadly reflecting the main evaluation questions of the Fitness Check.

A more detailed overview of the interview programme is presented below:

[223] This is the sum of those who answered "often" and "some of the time".
[224] This is the sum of the replies “always” and “some of the time”.
[225] This is the sum of those who answered "regularly" and "several times".
[226] This is the sum of those who mentioned a "moderate level" of distress and "quite a lot of distress".
[227] This is the sum of those who indicated "some level" of knowledge and "sufficient knowledge".

Category of interviewee	Completed
Consumer associations	11
EU policymakers (including those responsible for enforcement and the CPC Network/Regulation)	3
Legal researchers and academics	19
National enforcement authorities	6
National Ministries[228]	30
NGOs	1
Online marketplaces	3
Online platforms	2
Software / search engines/ app producers/ AI developers	2
Other individual traders	4
Trader associations (representing different industries e.g. digital-focused associations, representatives of doorstep selling)	20
Total	**101**

Most of the views expressed were in line with the responses to the other consultations:

- Traders and business associations stressed that the existing rules should be enforced to their fullest extent before proposing any legislative changes. There were calls for better implementation of existing EU consumer law before any revision of the legal framework, especially given the recent amendments by the MD.
- Consumer association raised the risk of information overload, though also welcoming increased transparency for online platforms through the MD and information disclosure requirements pertaining to who is the seller, as this will help consumers to understand if the seller is really in a third country and to make more informed purchasing choices.
- The importance of investing in tools that protect consumers, especially minors, was stressed by a major digital platform.
- Restrictions against the requirement to provide credit card details for free trials was also raised, as some stakeholders were concerned that this could lead to unintended consequences, namely that traders could become more reluctant to offer free trials.
- Highlighted the issue of hidden influencer marketing of risky financial products, gambling, sports betting, medical products and services.
- The expanding list of information obligations can be burdensome, particularly to SMEs, who are less able to keep up with the changes resulting from different legal instruments, including sector-specific legislation going beyond the three Directives.
- When entering another Member State's market, traders reported having incurred additional compliance costs regarding the rules on pre-contractual information, advertising/marketing and standard contract terms.
- Feedback points to challenges in bringing enforcement actions due to the complexity of the complaints and the underlying technologies as well as the fact that digital-related strategic deterrent cases often include concurrent breaches of other digital and data laws.

[228] Interviews with Ministries were undertaken for the Modernisation Directive part in all Member States and some Ministries were also interviewed separately regarding the Fitness Check part. In some countries, such as Denmark, more than one Ministry was interviewed as different Ministries are responsible for the transposition of different consumer law Directives.

- Feedback highlighted a concern for some traders about having to inform consumers about their right of withdrawal from contracts for digital content, only to have them immediately waive that right, which may create a negative perception for the consumer and therefore traders find it better to allow cancellations and refunds at any time.
- National authorities and consumer organisations highlighted some of the challenges concerning the regulation of scalping practices, such as defining the scope of scalping, determining permissible resale prices and practical enforcement difficulties given the cross-border nature of scalping activities.

Events and meetings

A **Member State expert group on consumer and marketing law** (including EU27 and EEA countries) was consulted during two meetings on 3 June 2022 and 20 October 2023.

A stakeholder expert group, the **Consumer Policy Advisory Group**, was consulted during two meetings on 21 April 2022 and 29 November 2023.

Information about these groups and the minutes of the meetings are publicly available in the register of Commission Expert Groups.

During the Fitness Check, DG JUST also held a number of **bilateral and multilateral meetings** with stakeholders, at their request, to further explain the aims of the Fitness Check and to gather additional views.

In addition to expert exchanges at the annual **European Consumer Summit**, DG JUST held three editions of the **Annual Digital Consumer Event** that enabled a public debate on specific topics relevant for the Fitness Check on 25 November 2021, 21 November 2022 and 30 November 2023. Each event included panels with representation from a consumer organisation, industry association, national authority and an academic expert. The events were streamed online to the public and it was possible for the audience to submit written questions to the panellists and to vote on questions raised.

The first edition was held prior to the formal launch of the Fitness Check and it included early reflections on whether EU consumer law, in its current form, suffices to ensure digital fairness. Panellists highlighted the changes in market developments, such as increased personalisation, the evolution of social media commerce and the use of more effective persuasion, as well as called for more clarity on the practices that are prohibited and pointed at the limits of relying only on guidelines (referring to the Commission's guidelines which were adopted a month later).

The second edition included three panel discussions focusing on specific topics covered in the Fitness Check: 1) "Online consumer vulnerabilities: shedding light on dark patterns, personalisation and structural asymmetries", 2) "Online consumer purchases: challenges raised by digital subscriptions, virtual items and the addictive use of digital products", 3) "Online consumer contracts: mapping unfair contract terms and the lack of transparency". Several panellists did not consider consumer law to be sufficiently fit, especially in order to tackle the structural state of power imbalance between consumers and traders online. The panel included a first call for a 'Digital Fairness Act' as a legislative follow-up. Some panellists highlighted that a periodical update of the respective guidelines, both at EU and national levels, helps steering the business behaviour towards better compliance but notwithstanding this, more precise and targeted rules may be needed to ensure more effective consumer protection. The panellists considered that the Fitness Check should focus on dark patterns, the fairness of interface design, preventing abusive personalisation

and revisiting the concept of average consumer. Another common theme was the importance of effective enforcement.

The third edition included two panel discussions focusing on specific topics covered in the Fitness Check: 1) “Burden of proof in consumer law”, 2) “Addictive design on digital services”. Some panellists emphasised that digital markets and complex technologies create information asymmetries between consumers/enforcers and traders, which can be remedied through evidence disclosure and burden of proof alleviation. The panellists discussed the approach to burden of proof in the revision of the Product Liability Directive, case law on medical malpractice and the Sale of Goods Directive. Some panellists emphasised the importance of legal certainty, so that the procedure is clear and predictable, while considering also the interests of SME-s with limited resources. There were explanations provided on how design techniques can exploit psychological traits and how addictive design differs from dark patterns. It is necessary to not only look at design features and interface, but also at the whole system architecture. To address complex challenges such as addictive design or the protection of minors, there is a need for a holistic approach that takes into consideration different stakeholder views and covers different legislation and disciplines.

Annex VI. Analysis of problematic practices

VI.1. Problematic practices

The success of the three Directives in achieving their objectives was analysed through specific case studies of the main problems identified in the Fitness Check, with a focus on the 'effectiveness' and 'coherence' criteria, as well as the 'relevance' criteria and the remedial measures suggested by stakeholders. The final selection of problems is based on the Commission's assessment, taking into account the frequency with which the problems were mentioned by stakeholders in the consultations, the availability of evidence and relevance for the material scope of the Directives.

VI.1.1. Dark patterns

Problems with dark patterns

The term dark patterns (or deceptive design) refers to commercial practices deployed through the structure, design or functionalities of digital interfaces or system architecture that can influence consumers to take decisions they would not have taken otherwise, e.g. presenting choices in a non-neutral manner, using fake countdown timers to create urgency, using emotional manipulation to make consumers second-guess their indicated choice, phrasing questions using double negatives, misleading consent options, e.g. in cookie banners.

Although traders' attempts to influence consumer decision-making is not a new phenomenon, concerns have intensified about the increased effectiveness and scale of such practices as well as the potential for personalised persuasion based on behavioural data. During the evaluation period, dark patterns have become **highly prevalent**, as evidenced by numerous studies and enforcement investigations from recent years, covering tens of thousands of websites and apps. The Commission's 2022 dark patterns study showed that 97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern, with the most common ones involving hiding information, creating false hierarchies in choice architectures, repeatedly making the same request, difficult cancellations and forced registrations.[229] The prevalence levels were similar in mobile apps and websites, across Member States and when comparing EU and non-EU traders, which indicates broad adoption, without distinction between sectors or the geographical coverage. The 2022 CPC sweep by EU/EEA consumer authorities found that nearly 40% of online retail shops contained at least one dark pattern, specifically fake countdown timers, hidden information and false hierarchies in choice architectures. The OECD's 2022 report on dark patterns provides further insights concerning their prevalence and effects on consumers, and a 2021 study by the Swedish authority reflects on some of the challenges from the perspective of policymakers and regulators. The 2024 International Consumer Protection and Enforcement Network (ICPEN) and Global Privacy Enforcement Network (GPEN) sweep of the websites/apps of 642 traders found that 75,7% of them deployed at least one dark pattern, and 66,8% of them employed two or more dark patterns. Sneaking practices (e.g. inability of the consumer to turn off auto-renewal of subscription service)

[229] The prevalence of specific types of dark patterns varied between different types of websites and apps. For example, countdown timers or limited time messages were quite prevalent on e-commerce platforms, while the use of nagging was more customary in health and fitness websites and apps.

and interface interference (e.g. making a subscription that is advantageous to the trader more prominent) were encountered especially frequently.

Dark patterns can affect a wide range of transactional decisions and many of them have been **empirically proven to appreciably impair the consumers' ability to take an informed decision**. In the public consultation, 89% of consumers reported being **confused by dark patterns** in website/app design and 76% **felt pressured** to buy something due to the language or design that was used. BEUC's 2023 survey found that 61% of consumers have felt under pressure when buying online and 41% **ended up buying things they did not intend to** due to confusing design. The Commission's 2022 dark patterns study included behavioural experiments with a sample of 7430 consumers in six Member States (BG, DE, IT, PL, ES, SE) which showed that when exposed to dark patterns the **probability of making a choice that was inconsistent with the consumers' preferences increased** – the average figure rising to 51% for vulnerable consumers and 47% for average consumers. Older consumers and those with lower education levels were more impacted. In an additional behavioural experiment, consumers that were exposed to a personalised 'forced action' dark pattern reported **higher levels of frustration and feeling of being manipulated**, compared to the control group that was not exposed to this dark pattern. Additionally, they showed a lower understanding of the information that was presented, perceived information on the website to be less transparent and the websites to be less trustworthy. A lab experiment also tested consumers' neurophysiological and psychological reactions to dark patterns, showing that the dark pattern hampered the participants' ability to take a decision and increased their heart rate, which is associated with increased anxiety and alertness.

The consumer survey conducted for this Fitness Check showed additional evidence of consumer experiences with the following practices that could be qualified as dark patterns, depending on the circumstances:

- The design or language used on a website or app was confusing, which made the consumer uncertain about what they were signing up for, or about which rights and obligations they had (40%).
- The consumer paid more than they planned to because, during the purchasing process, the final price changed to a price higher than the one advertised initially (32%).
- The website or app kept repeatedly requesting the consumer to make a decision, e.g. to get a premium account, offering special discounts, asking to buy a recommended product (48%). This response was particularly high among the younger age groups (36% of 18-25-year-olds; and 31% of 26-35-year-olds, compared to 12% of 56-65-year-olds and 11% of those aged 65+).
- The design or language used on a website or app made them feel pressured to buy something (35%).
- After indicating their choice or declined a choice offered, there were messages on the website or app that made them doubt their decision, e.g. asking questions like 'are you really sure you do not want a discount?' (42%).
- Important information was visually obscured or ordered in a way to promote an option that did not seem to be in their interest (37%).
- The labels used by search providers (e.g. online marketplaces or comparison tools) to distinguish sponsored search results from natural search results were not very clear (48%).
- There were preselected options that were in favour of the company but changing those options was difficult (37%).

- Making a choice (such as clicking a button or hyperlink) led to a different result than they would normally expect, e.g. clicking an unsubscribe button led to a page describing the benefits of that service that the consumer would lose (42%).
- The design or language used on a website or app made it difficult to understand how to exercise their consumer rights, e.g. to make a complaint or receive compensation (40%).
- There were claims that a product was low in stock or high in demand, e.g. that many other consumers are currently looking at the same product (66%). This practice was identified most often by those who often engage in gambling or games of chance: 42% by those who engage in this activity daily and 39% by those who engage several times a week encountered such messages regularly.
- There were claims that a product was available only for a limited time, e.g. countdown timers running for a few hours (61%).

Legal framework

The legal provisions in the Directives under evaluation **only partly address dark patterns**. In 2021, the Commission adopted an updated UCPD Guidance to further explain how to apply the rules to dark patterns. Under the UCPD, regardless of the trader's intention, a manipulative practice that materially distorts or is likely to distort the economic behaviour of an average or vulnerable consumer could breach the trader's professional diligence requirements or amount to a misleading or aggressive practice (e.g. creating obstacles to contract termination or switching by means of confirmshaming is potentially aggressive), depending on the specific dark pattern applied and subject to a case-by-case assessment by national courts or authorities. Only a limited number of dark patterns are directly prohibited in the UCPD blacklist, although **none of the existing prohibitions refer specifically to digital interfaces and their application hinges upon a case-by-case assessment**. Examples of prohibited practices include 'bait and switch' (offering products at a specified price while not disclosing the existence of reasonable grounds for not being able to provide the product or refusing to take orders for it or deliver it within a reasonable time, with the intention of promoting a different product instead); fake urgency (falsely stating that a product will only be available for a very limited time or on particular terms for a very limited time); misleading availability claims (inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to buy the product at less favourable conditions); fake prizes (claiming that the consumer has won a prize, without awarding the prizes described or a reasonable equivalent), misleading 'free' claims (falsely describing a product as 'free' if the consumer has to pay anything other than the unavoidable costs related to responding, collecting or delivery); sneaking into basket (demanding immediate or deferred payment for or the return or safekeeping of products supplied by the trader, but not solicited by the consumer) and unwanted solicitations (making repeated intrusions during normal interactions in order to get the consumer to do or accept something).[230]

Dark patterns that involve hiding information could amount to misleading actions or omissions under the UCPD, based on a case-by-case assessment. However, the lack of legal certainty about the fairness or unfairness of specific types of dark patterns under the UCPD could undermine the effectiveness of its application. In addition, the CRD specifically prohibits traders from using pre-ticked boxes or other default settings that the consumer has to reject in order to get the consumer's consent specifically for any additional payments. The CRD also exempts the consumer from any obligation to pay in case of

[230] Points number 5, 6, 7, 18, 19, 20, 26, 29 and 31 of Annex I to the UCPD.

unsolicited supply (which is prohibited by the UCPD and could also take the form of sneaking additional items into the online shopping basket). The UCTD requires standard contract terms to be drafted in plain intelligible language. If the transparency of the term is undermined by the use of dark patterns, then it could be rendered unfair, and if it led to interpretative ambiguities about the meaning of a term, then the interpretation that is most favourable for consumers should prevail. Only a limited number of contract terms that entail dark patterns are indicated as potentially unfair in the UCTD indicative list[231], subject to a case-by-case assessment by national courts and authorities.

Despite the increased attention given to the topic, case law applying the Directives to dark patterns has been limited so far. Notable examples include the 2020 CPC coordinated action concerning accommodation booking platforms Booking.com and Expedia, which led to improvements regarding the accuracy of time-limited offers and claims about the number of consumers that are allegedly looking at the offer simultaneously or the diminishing number of rooms left. In 2022, CPC authorities took another action concerning the difficult cancellations of Amazon Prime (see the subsequent section on digital contract cancellations). In 2024, the Polish authority fined Amazon for using dark patterns, including false or misleading information on product availability and delivery times.

According to several stakeholders and authorities, enforcement actions can be more effective if courts and authorities are able to point to specific practices in the UCPD blacklist. Furthermore, clearly formulated dark patterns prohibitions can be more suitable for automated enforcement checks. For example, in 2023, the Dutch authority took action against fake countdown timers following an automated check of thousands of online shops.

The Fitness Check also inquired about the use of the **aggressive practice** legal basis in the UCPD, which goes beyond merely misleading consumers or distorting information. The UCPD regards a commercial practice as aggressive if by harassment, coercion, or undue influence it significantly impairs the consumer's freedom of choice or conduct to distort their decision-making. The provisions contain several factors that can be taken into account, such as the exploitation by the trader of any foreseeable and specific misfortune or circumstance about the consumer. Harassment and coercion are not defined, whereas 'undue influence' is explicitly defined as exploiting a position of power on the consumer to apply pressure, even without using or threatening to use physical force, in a way that significantly limits the consumer's ability to make an informed decision.

This prohibition of aggressive practices, which was initially meant to address offline scenarios, could be considered from a new perspective in the digital age. However, the CJEU has issued only three rulings on aggressive practices and just one of those cases concerns a digital scenario.[232] National case law is similarly scarce. In the UCPD Guidance, the Commission has pointed in particular to 'undue influence' as a relevant indicator of an aggressive practice when the trader is using information about consumer vulnerabilities for commercial purposes. However, the guidance is non-binding and the **legal basis remains largely unexplored through enforcement** (see the supporting study for further information).

[231]Examples of unfair terms in the UCTD indicative list include forced continuity (automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early) and forced registration (irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract). Points (h) and (i) of Annex to the UCTD.

[232] C-102/20 StWL Städtische Werke Lauf a.d. Pegnitz, which concerned the interpretation of UCPD Annex point 26 on persistent and unwanted solicitations, as applied to "inbox advertising".

A recent case law example concerns BEUC's 2021 complaint about Whatsapp's practices regarding the recurring prompts to consumers to accept changes to T&Cs, which they considered to amount to aggression, given the nature, location, timing and persistent nature of the prompts. Although the subsequent CPC coordinated action succeeded in obtaining commitments from Whatsapp to stop and remedy the unfair practices, it did not clarify whether those practices were considered aggressive by the authorities. Other notable examples concern the Italian authority's 2018 action against Facebook for exerting undue influence on consumers through pre-selected choices regarding the transmission of their data to third parties for targeted ads and the 2021 action against Google and Facebook concerning similar aggression to induce data sharing for commercial purposes.

Several stakeholders and academics argue that, despite its potential, the 'aggressive practice' legal basis is not sufficiently effective in achieving their objectives in the digital context. The Fitness Check found that one reason for this is that most Member States were unfamiliar with aggression as a legal basis in consumer protection prior to the introduction of the UCPD. There is a need for more legal certainty on concepts like harassment, coercion, undue influence, position of power and significant impairment. It is notable that this legal basis could be relevant for tackling multiple problems explored in the Fitness Check, including dark patterns, addictive design, manipulative personalisation and aggressive cases of influencer marketing.

Concerning coherence with new legislative developments, the 2023 revision and repeal of the DMFSD introduced in the CRD Article 16e with an obligation for Member States to ensure that traders do not apply dark patterns when concluding financial services contracts at a distance. It also gave the Member States a choice to adopt specific measures to address at least one of the three dark patterns listed therein and allowed them to maintain or introduce more stringent protections regarding dark patterns in this area (minimum harmonisation). Given that the scope of the obligation is limited to financial services and to the conclusion of contracts, there is **no equivalent protection for products and services other than financial services, and regarding transactional decisions outside of the contract conclusion stage**.

This is complemented by Art. 25 DSA, which prohibits online platforms from deploying dark patterns and indicated three examples of such practices, notably the distortion of choices, nagging and difficult cancellations. The scope of the DSA prohibition explicitly excludes practices 'covered by' the UCPD and GDPR[233]. Taking into account the broad scope of the UCPD, which covers virtually all B2C commercial practices in the advertising, sales or after-sales stages, the DSA prohibition is therefore likely to have limited relevance for regulating B2C dark patterns. On 18 December 2023, the Commission relied on this legal basis in the opening decision against the platform X (notably in relation to checkmarks linked to certain subscription products). There is considerable doubt among stakeholders and academics about the exact meaning of practices that are 'covered by' the scope of the UCPD. Many consider that enforcement authorities would face considerable risks when bringing forth actions invoking Art. 25 DSA. For this reason, the interplay between this DSA provision and the UCPD was among the **most common coherence problems reported by stakeholders in the Fitness Check consultations**.

[233] Regarding deceptive design under the GDPR, see the EDPB guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

The DSA contains additional provisions that would allow addressing certain concerns related to dark patterns. First, the DSA's compliance by design provision requires online marketplaces to design their interfaces in a way that enables traders to comply with their information obligations under consumer law, which could be used to scrutinise certain dark patterns that involve hiding information. Secondly, when it comes to VLOPs and VLOSEs, the risk assessments and mitigating measures that the DSA requires is a means to address certain dark patterns. For example, on 19 February 2024, the Commission adopted an opening decision against TikTok, relying on the provisions on risk assessment, pointing to the lack of assessment of actual or foreseeable negative effects stemming from the design of TikTok's system that may stimulate behavioural addictions. However, it should be noted, that the DSA has a different scope from the horizontal consumer acquis. Art. 25, for instance, applies to online platforms, but not small or micro enterprises, search engines, individual traders that do not qualify as intermediaries and various digital services whose platform-like features are merely ancillary to the principal service (e.g. video games). It therefore does not provide a comprehensive framework to address the identified problems related to dark patterns.

Additional dark pattern prohibitions were introduced in legislation with more specific material scopes. The AI Act prohibits specific use cases 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, which leads or is (reasonably) likely to lead to significant harm. The application of these prohibitions is dependent on the interpretation of specific terms (such as 'subliminal technique' and 'purposefully' manipulative or deceptive), the resulting harm must be considered as significant and not all types of vulnerabilities are covered. The Data Act prohibits third parties that receive consumer data from connected products or services from making it unduly difficult through dark patterns for consumers to exercise their relevant rights or choices. The DMA includes an anti-circumvention clause that prohibits designated gatekeepers from circumventing the obligations in the DMA through contractual, commercial, technical or any other means, which includes the use of dark patterns to unfairly steer consumer decisions. As we enter into the implementation phase of these different new regulatory regimes, it is likely that future case law developments, guidelines and standards that interpret the proliferation of different terms used in these new legal acts, such as 'coerce', 'deceive', 'undermine', 'manipulate', 'subvert', 'impair' and 'materially distort', will impact on the application of EU consumer law. In this context, it will be of key importance to ensure a coherence application of the rules over time.

Stakeholder views

Concerning possible solutions to the identified problems, 62% of stakeholders in the public consultation supported **introducing clearer and stronger protections** against dark patterns and similar manipulative practices. Based on the consultations and data collection, stakeholders have raised concerns around legal uncertainty and complexity, ineffective enforcement and potential incoherence. This could be alleviated through the **concretisation of dark patterns prohibitions in the UCPD**, including by adapting existing prohibitions and adding new additions to the blacklist that are specifically addressing online interfaces, such as:

- Pressuring the consumer during the booking process through urgency and scarcity claims (in certain cases, even if the claims are truthful).

- Using misleading or ambiguous language in the presentation of choices to consumers, such as reversing the linguistic or framing logic within a list of choices, using double negatives.
- Pressuring or shaming the consumer toward a particular choice through emotive language or framing (confirm-shaming).
- Repeatedly requesting or urging the consumer to make a choice, such as take a transactional decision, agree to changes in contract terms or change their previously established preferences (nagging).
- Adding new charges to the total price when a consumer is about to complete a purchase during the booking process (drip pricing).
- Adding new products or services to the shopping basket when a consumer is about to complete a purchase during the booking process (sneak into the online basket).
- Creating different lengths of click paths to different options in order to steer consumers to choose the path preferred by the business to the detriment of the consumer (click fatigue).
- Making the process of cancelling a contract disproportionately onerous, complex or time-consuming.
- Making the indicated choice lead to a different result than normally expected by the consumer.

Some stakeholders, in particular consumer organisations, considered that the legal framework could also be more prescriptive with a cross-cutting prohibition of deploying dark patterns and about the factors that should be taken into account in the assessment, such as the combined effect of deploying multiple dark patterns in the consumer's transactional journey and the extent to which behavioural data was used to personalise or otherwise increase the effects of dark patterns. More generally, it is suggested, it could be expressly clarified that practices involving psychological pressure and attention capture are covered by the material scope of the UCPD.

In addition, stakeholders consider that the effectiveness of the UCPD's provisions on aggressive practices could be enhanced by providing more legal certainty on its key concepts (harassment, coercion, undue influence, position of power, significant impairment).

It is also suggested that dark patterns that involve impediments to switching and contract cancellations could additionally be remedied by prescribing easier and clearer mandatory cancellation functions, similarly to the withdrawal function for the 14-day right of withdrawal that was introduced in the CRD following its recent amendments related to the DMFSD.

An additional measure suggested by some stakeholders is the imposition of a 'fairness by design' duty on traders, which would entail the introduction of technical and organisational measures to incorporate consumer protection considerations at all stages of the product or service development, similarly to the requirement of data protection by design and by default in Art. 25 GDPR and the compliance by design requirement in Art. 31 DSA. Furthermore, several stakeholders suggest that the effectiveness of the Directives could be increased through the introduction of an 'anti-circumvention' rule, similarly to Art. 13 DMA, which makes explicit reference to interface design.

Dark patterns were also brought as an example of the type of problem that may warrant the alleviation of the burden of proof concerning the trader's practices regarding the online choice architectures they created.

Possible non-legislative measures suggested by stakeholders include the further updating of the Commission's guidelines to provide more legal certainty and coherence with other legislation, the facilitation of more consistent enforcement, including through enforcement guidelines and checklists that traders can use to audit their interface designs, developing automated enforcement tools, incorporating more behavioural insights, creating a European database of dark patterns, and requiring annual reports from enforcement authorities about actions taken against dark patterns.

To conclude, based on stakeholder input and data analysis, EU consumer law does not appear to be sufficiently clear or effective in tackling dark patterns, which undermines the effective implementation of several EU consumer rights and puts into question the ability of the average or vulnerable consumer to take informed transactional decisions in the digital environment.

VI.1.2. Addictive design and gaming

Problems with addictive design

The Fitness Check identified concerns about interface designs and functionalities that **induce digital addiction** (addictive design or, alternatively, attention-capture dark patterns). It is generally in the traders' economic interest to design their products in a manner that **increases the amount of time, money and engagement** that consumers spend, especially those traders whose business model relies on the processing of consumer data. However, the addictive use of digital products and services carries the risk of economic, physical and mental harm, including, but not confined to, vulnerable consumers such as children (see further information in the 'digital addiction' case study in the supporting study). Addictive design has started to receive attention from the consumer protection perspective, as most of the problematic practices in question are directly connected to the traders' commercial incentives and the consumers' transactional decisions.

A 2019 study by the European Parliament Research Service reviewing empirical research indicates that digital addiction affects millions of EU consumers.[234] In the public consultation on the Fitness Check, 33% of consumers reported **spending too much time or money** using certain websites or apps. Likewise, in the consumer survey, 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, whereas 24% had no experience with this type of situations. BEUC's 2023 survey found that 83% of consumers report spending more time on social media than they intended.

Digital addiction is currently not listed among substance-related disorders (e.g. smoking, alcohol), behavioural disorders (e.g. pathological gambling) or as a diagnosis in standard classifications.[235] Only gaming addiction has been formally recognised as a disorder in 2013. The EP's 2023 resolution on addictive design of online services highlighted the

[234] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624249/EPRS_STU(2019)624249_EN.pdf

[235] Not listed in the Diagnostic and Statistical Manual of Mental Disorders (DSM-V) or the International Statistical Classification of Diseases and Related Health Problems (ICD-10/ICD-11).

negative impact that addictive design could have on consumers.[236] Concerns are raised with regard to features such as the automatic playing of new content (**autoplay**), allowing the consumer to 'pull' an interface to manually reload the system for new content (**pull-to-refresh**), the elimination of natural stopping points by showing new content automatically and continuously as the consumer scrolls down (**infinite scroll**), content that is temporarily available (**ephemeral content**), various **incentives for continued engagement** (e.g. badges, rewards) or, conversely, **penalties for disengagement**. Concerns have also been raised more generally with **interaction-based recommender systems and notifications** that are delivered during or outside of the consumer's interaction with the digital product or service, as well as with **gamification**, which entails the integration of game-like elements in non-gaming environments.

Legal framework regarding addictive design

The general provisions of the UCPD could capture some of these practices or scenarios, subject to a case-by-case assessment by national courts and authorities, such as when the trader is exploiting a known vulnerability (e.g. lack of impulse control, gambling history) in deploying addictive design to unduly influence the consumer's decision. The Commission's UCPD Guidance gives examples of 'addictive interface designs' in the context of gaming, which could indicate the risk of an unfair practice in certain circumstances, namely slot machines designs, loot boxes, betting, offering micro-transactions during critical moments in the game, pervasive nagging, or the use of visual or acoustic effects to put pressure on the consumer to engage in further expense.

However, the legal provisions of the three Directives would be difficult to apply to some other specific aspects of addictive design related to time loss and mental harms. Such broader harms from digital addiction are even perceived by some stakeholders as new territory for EU consumer law, considering that it is concerned with the protection of the economic interests of consumers that is generally understood as safeguarding their material welfare. In contrast, the objective of the recently adopted General Product Safety Regulation (GPSR) is to protect the health and safety of EU consumers. The GPSR strongly underlines that 'health' is to be seen as a state of complete physical, mental and social well-being, and not merely the absence of disease or infirmity. Capturing addictive design would depend on the interpretation of the economic interest concept as covering also consumer's time and negative consequences to their mental health, which indirectly and/or eventually would also affect the consumers' material welfare.

The UCPD Guidance already highlights the Commission's interpretation of the broad scope of the legal concept of a consumer's 'transactional decision', which includes not only purchasing decisions but also decisions to continue using the service, such as scrolling, which are relevant for attention capture practices. However, this interpretation of the 'transactional decision' is not reflected expressly in the legal provisions and there have been diverging national rulings, e.g. the Federal Supreme Court of Germany would not consider a decision to take a closer look at an offer in an advertisement or clicking on a social media post referencing a trader through the 'tap tag' to be a transactional decision.[237]

In the absence of specific provisions in EU consumer law or other EU legislation, there is **legal uncertainty** about the deployment of certain features that are described as addictive

[236] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2023/2043(INI)
[237] Federal Supreme Court, decision of 18 December 2014, I ZR 129/13, Schlafzimmer komplettn; and decision of 9 September 2021, I ZR 90/20, Influencer I.

design. Case law and enforcement activities in this context are very limited, but exploratory cases have started to emerge in 2024.

In March 2024, the Italian authority fined TikTok[238] for UCPD breaches that relate to addictive design features, in particular the recommender system, but the decision also addressed broader questions concerning the platform's responsibility in the dissemination of harmful content, especially to adolescents. The decision qualified addictive design practices as aggressive, amounting to an undue influencing of users and exploiting the vulnerabilities of certain groups.

The DSA has brought important changes, strengthening the protection of minors on online platforms and social media in particular. Key provisions include the ban of personalised advertising towards minors, mandating platforms to take 'appropriate and proportionate measures' to protect minors (e.g. designing their online interfaces with the highest level of privacy, safety and security by default; with standardisation to be promoted) and explaining the conditions for the use of the service to minors. In addition, the risk assessments and mitigation that VLOPs and VLOSEs are obliged to undertake expressly cover risks to the rights of the child (e.g. including exposure to content that may impair their mental health and online interfaces that may be addiction-inducing). It covers concerns regarding digital addiction in the context of the systemic risks to a high level of consumer protection and when it comes to serious negative consequences to a person's physical and mental well-being. However, it should be noted that the scope of these provisions does not cover traders that do not qualify as intermediaries or traders providing digital services such as video games whose platform-like features are merely ancillary to the principal service or streaming services that qualify as non-linear media service providers.

In February 2024, the Commission opened formal proceedings against TikTok[239] under the DSA. The grounds for the proceedings include compliance with the DSA obligations related to the assessment and mitigation of systemic risks, in terms of actual or foreseeable negative effects stemming from the design of TikTok's system, including algorithmic systems, that may stimulate behavioural addictions and/or create so-called 'rabbit hole effects'. The press release clarified that such assessment is required to counter potential risks for the exercise of the fundamental right to the person's physical and mental well-being, the respect of the rights of the child as well as its impact on radicalisation processes. Furthermore, it was noted that the mitigation measures in place in this respect, notably age verification tools used by TikTok to prevent access by minors to inappropriate content, may not be reasonable, proportionate, and effective.

In April 2024, the Commission opened second formal proceedings against TikTok[240] under the DSA, specifically regarding the launch of TikTok Lite in Spain and France, which included a Task and Reward Program allowing users to earn points and rewards (monetizable in-app currency, Amazon vouchers, PayPal gift cards) while performing certain tasks on TikTok, such as watching videos, liking content, following creators, inviting friends to join TikTok etc. The Commission was concerned that there had not been a proper risk assessment and risk mitigation of such features. Following the opening of the proceedings, TikTok voluntarily suspended the service.

[238] https://www.agcm.it/media/comunicati-stampa/2024/3/PS12543-
[239] https://ec.europa.eu/commission/presscorner/detail/en/IP_24_926
[240] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227

The AI Act could limit certain addictive design features that involve the use of AI if they cross the threshold of purposefully manipulative or deceptive techniques or exploiting the vulnerabilities of persons related to their age, disability or a specific social or economic situation, and if it leads or is (reasonably) likely to lead to significant harm. It is not evident whether addictive design functionalities could cross this high threshold.

Legal initiatives in other jurisdictions have been rare so far. For example, a 2019 proposal in the US (not adopted) for the Social Media Addiction Reduction Technology (SMART) Act suggested banning infinite scroll, the elimination of natural stopping points, autoplay and achievements for continued engagement. In October 2023, several Attorney Generals filed a federal complaint against Meta, alleging that the company was misleading about the safety of their services, which are designed to induce addiction and violate children's privacy.[241]

Problems with virtual items and in-app currencies

Problems have also increased with specific products such as video games and social media that increasingly involve the **sale of virtual items** (e.g. gifts, power-ups, cosmetic features), including those with uncertainty-based rewards (e.g. loot boxes, card packs, prize wheels, access to levels that have a chance of finding rare items), and the use **intermediate in-app virtual currencies** (e.g. coins, gems, bucks, credits). The providers whose business model is based upon or includes the sale of in-app purchases require the users to first buy the in-app currency that they use afterwards to make in-app purchases. Many stakeholders are concerned that such payment system distorts the real value of the in-app transaction for consumers and encourage them to spend more than they intended.

Video games and gaming platforms are increasingly a commercial environment for children, which raises different concerns. BEUC's 2023 survey found that 59% of consumers play online games or visit other websites where they can buy virtual items in exchange for real money and 80% of them were prompted to spend money on virtual items. In the public consultation, 47% of consumers reported being **confused about the real price of virtual items.** In the consumer survey, 29% of consumers had experienced a situation where the real price of a virtual item was not clear because it was only indicated in the app's virtual currency. This was particularly high amongst those consumers who indicated that spending time online negatively affects their daily life (48% had regularly experienced this). On a country level, this was particularly common for consumers from Romania (25%) Hungary (24%) and France (23%). 25% of consumers in BEUC's 2023 survey considered that the chances of getting a desired reward from a loot box were not sufficiently specified in the games they played and 23% considered that the real price of virtual items was not clearly indicated.

A 2023 study commissioned by Norway[242] examined three popular video games, which contained multiple virtual currencies and up to 11 470 different products in the object inventory, showing that in-game virtual item offers are expanding, even on a daily basis. The study identified 13 possible dark patterns or addictive design elements, which concern visual design, unclear labelling, time-based elements (e.g. daily rewards, streaks, countdowns) and gambling-style mechanisms (e.g. loot boxes, wheels of fortune, free samples). Interviews conducted with children for the study showed that purchasing in-game content has an important social function and that children can be influenced by

[241] https://ag.ny.gov/sites/default/files/court-filings/meta-multistate-complaint.pdf
[242] https://oda.oslomet.no/oda-xmlui/handle/11250/3101047

different game designs to spend more time and money than planned. However, children also adopt different strategies to resist commercial content and manipulative design.

The Fitness Check consultations also pointed to concerns about the **marketing practices** related to virtual items, such as **bundling and pricing presentation** (e.g. currencies can only be bought in larger quantities in bundles, while a specific virtual item costs less, resulting in left-over currency; necessity to buy a 'key' to open a loot box), **'pity timers'** that increase the odds of winning after many losses and **pay-to-win** models, including features that offer the possibility to **pay to remove pressure** or to **skip forced waiting**.

Additional concerns were raised regarding video game providers that **stop the provision of the game**, which leads to the loss of access to the game and to any virtual items purchased.

Furthermore, there are significant concerns about **virtual items with uncertainty-based rewards**, especially **loot boxes**, which some stakeholders qualify as harmful features that encourage gambling and impulse buying, and **skin gambling/betting** whereby players wager in-game items on the outcome of video games played within competitive multiplayer environments.[243]

The EP's 2020 study on loot boxes highlighted the existing research on the effects of loot boxes and recommended to broaden the policy perspective beyond gambling aspects towards a wider consumer protection angle.[244] Several Member States have taken steps to address loot boxes, such as considering prohibiting them for minors (ES) or qualifying them, under certain conditions, as a 'gambling service' that is subject to the oversight of gambling authorities (BE, NL), but there continues to be considerable ambiguity at national level. For example, in a 2022 ruling a Dutch administrative court overruled an infringement decision by a gambling authority that qualified loot boxes (packs) in FIFA22 as a 'game of chance'.[245] Several jurisdictions do not consider features like loot boxes as gambling due to the impossibility of 'cashing out' in real currency (i.e. the content has no economic value outside of the game) or transferring it to other players. In these conditions, stakeholders call for the focus to shift to consumer protection laws, as also recommended in the 2020 EP study on loot boxes. The UK government conducted a call for evidence in 2022 and convened a working group of game industry representatives to discuss protections for children and loot boxes, which resulted in industry guidelines in 2023.[246] The guidelines include a commitment to restrict minors from acquiring a paid loot box without the consent or knowledge of a parent or guardian and setting default spending limits on child accounts.

A 2023 sweep conducted in the Fitness Check's supporting study examined different issues in the context of video games, including the adequacy of the information disclosure, right of withdrawal and the presence of any problematic practices. The sweep primarily illustrates the variety of approaches taken by video game providers within the current framework of consumer laws, industry self-regulation and guidelines:

- The price of the game was clearly stated up-front for PC games, but less so for mobile games (92.3% PC, 57.1% mobile), with slightly lower figures for clarity in case the game is labelled as 'free' (90.9% PC, 45.5% mobile).

[243] The buying of items like loot boxes and participation in skin gambling have been shown to cause adverse effects for minors, including financial and mental harm, however, the 2020 EP study on loot boxes notes that there is no consensus on the causal link between loot boxes and harmful effects.
[244] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU(2020)652727_EN.pdf
[245] https://www.raadvanstate.nl/@130206/dwangsom-onterecht-opgelegd-loot-boxes/
[246] https://www.gov.uk/guidance/loot-boxes-in-video-games-update-on-improvements-to-industry-led-protections

- Upfront information about the presence of in-game purchases was provided in around half of cases (53.8% PC games, 42.9% mobile), whereas in fact 67.9% of the games included the possibility of in-game purchases.
- The prices of in-game purchases were presented in different ways – 26.3% only showed the price in the in-game currency, 15.8% only in the national currency and 57.9% presented the price in both currencies. One game had a clear separation between in-game currencies that can be obtained through purchasing with real currency and in-game currencies that can be obtained while playing.
- In 61.5% of cases where there was an in-game currency, the price of that currency per unit would decrease if the consumer would buy the currency in bundles, thereby encouraging consumers to buy more. The dynamics of the currency mechanisms could also be complex and difficult for the consumer to understand, e.g. in two cases, the available stock of currency earnable in the game increased as time goes by and the maximum value the player can hold could increase based on investments made using the currencies.
- Only in one third of cases, the right of withdrawal policy relating to the in-game purchases was presented, explaining that the consumer would have to consent to the loss of the right of withdrawal immediately following the acquisition of the in-game purchase.
- Loot boxes and similar virtual items (e.g. passes allowing players to access different levels of the game) appeared in 30% of cases and there was generally no clear information of what features they contained. However, no game included proactive promotion of loot boxes during the first 15 min of gameplay.
- Dark patterns such as nagging (19.2%), fake urgency (19.2%), social proof (11.5%), confirmshaming (7.7%) and hidden information/false hierarchy/trick questions (3.8%) were encountered in mobile games, but not in PC games.
- Other practices that could be qualified as potentially addictive design included incentives for continued playing or penalties for discontinuing the gameplay (prompts such as "if you quit now, you'll lose your active powerups"). In some games with a multi-player element, consumers were incentivised to log into the game at least once a day, otherwise they were at greater risk of suffering penalties (e.g. being attacked by other players), which could be avoided by buying virtual items (e.g. protective shields).
- Mobile games generally asked at the start of each session whether push notification could be allowed and, if accepted, consumers could be reminded on a daily basis about their progress or the benefits they could lose by not logging into to the game.
- In 38% of cases, consumers were encouraged to connect through a social media platform. The element of social media could also be linked to the gaming platform (e.g. the Steam gaming platform allows consumers to share their achievements with others through gaining ‘achievements’ or ‘badges’ that are displayed on their profile).
- Two games allowed to set a limit for a maximum amount spent through settings in the game. In one case, the controls allowed to disable features such a multi-player mode or set a cap on the amount of time played per week. One game allowed this to be done specifically by the parent linking their account to their child’s.

A 2024 study[247] examined the 50 highest-grossing games in the Apple App Store in the Netherlands from the consumer protection perspective, finding significant instances of non-compliance:

- Only 2% of games gave price in EUR for all in-game purchases observed.
- During up to one hour of gameplay, paid loot boxes were identified in 43 of the 50 games (86%). Only 11.6% of games with loot boxes sold them with a price in EUR.
- 100% of the games disclosed the presence of in-game purchases, but only a 4.7% disclosed the presence of loot boxes. In case the game contained in-game purchases, the games were not presented as 'free' in the mobile version of the Apple App Store, but such language remained in the desktop webpage version.
- 34.9% of games with loot boxes disclosed probabilities. However, only 9.3% of games with loot boxes disclosed probabilities for each individual virtual item. There were diverging approaches to disclosures, including unclear explanations such as showing all potential rewards as a question mark with a percentage value attached.
- 90% of games included commercial communications that could potentially be qualified as a direct exhortation towards children to buy products, depending on a case-by-case assessment by consumer authorities.

Legal framework regarding virtual items and in-app currencies

Concerning the applicable legal framework, the **sale of virtual items and the use of intermediate in-app currencies is allowed under EU consumer law**, provided that the related marketing practices are not unfair (e.g. UCPD Annex I point 28 prohibits direct exhortations towards children, which include claims such as 'buy now' or 'this character needs you') and the sale complies with the information obligations under the CRD and UCPD concerning the price and main characteristics of the product. Also **loot boxes and other virtual items with uncertainty-based rewards are not prohibited as such**. The determination of the existence and validity of contract, which triggers the application of consumer contract law requirements (specifically, information and formal requirements and the right of withdrawal under the CRD), is subject to national law. The treatment of the acquisition of virtual items with in-app currencies under national law requires a case-by-case assessment (e.g. determining whether these are separate contracts or part of the execution of an existing contract). This means that in some cases such acquisition is subject to the requirements of the CRD but not in others, i.e. the legal status of these transactions is not certain.

As also shown by the sweep findings, there is significant **lack of compliance with the Directive's provisions regarding transparency and right of withdrawal regarding virtual items and in-app currencies.** Although the Commission provided additional legal interpretation in the UCPD and CRD Guidances, there is no CJEU case law confirming it. The Commission considered in the Guidance that the prices of virtual items should be also expressed in real currencies (in addition to the price in in-app currencies) and that, in the case of virtual items with a randomisation element, there should be a clear explanation of the probabilities of receiving a random item. In contrast, video game representatives consider that the consumer's transactional decision happens at the moment they decide to purchase the in-app currency and the subsequent exchange of that in-app currency for virtual items is not commercial by nature and does not require parallel indication of the value in real currencies. They also point to the difficulties with estimating the value of the

[247] Xiao, Leon Y. "Failing to Protect the Online Consumer: Poor Compliance with Dutch Loot Box and Video Game Consumer Protection Guidelines." OSF Preprints, 6 May 2024.

virtual item in real currency in cases where it can be both bought and also earned in the game ('mixed pot' approach). In contrast, there are also games that do not use the mixed pot approach.

Industry self-regulation in this area, in particular the Pan-European Games Information System (PEGI), focuses on transparency obligations (e.g. on the presence of in-app purchases and gambling-like features such as loot boxes) and age-labelling, so that parents and children could make more informed decisions.

The Fitness Check consultations also raised questions about the legal qualification of the contracts for the purchase of in-app currencies and virtual items (i.e. whether it is a digital service, digital content or a digital representation of value, whether such items are sold or only licenced). Such a qualification is important for determining the applicability of specific consumer rights, in particular the 14-day right of withdrawal.[248]

Concerning the problems regarding the cessation of the provision of video games, leading to a loss of access to the game and to virtual items purchased, the Digital Content Directive stipulates that the consumer is entitled to have the online video game in conformity with the contract throughout the duration of its supply. In the event of termination of a contract for the supply of the video game over a period of time, the provider must reimburse the consumer for the part of the price paid in advance for any remaining period of the contract if it had not been terminated. However, consumer law does not currently set specific requirements as to the duration of the supply. The UCTD prohibits unfair terms causing a significant imbalance in the parties' rights and obligations to the detriment of consumers. Terms such as those related to the unilateral modification or termination by the trader of a contract of indeterminate duration without reasonable notice may be deemed unfair subject to a case-by-case assessment.

Case law and enforcement activities on virtual items and currencies have been limited. A recent example is the 2021-2022 CPC action on TikTok, which resulted in more transparency in the platform's policies about the purchase and use of 'coins', including a pop-up window with the estimated price in local currencies, how to get 'rewards' or send 'gifts', and consumers were allowed to withdraw from the purchase of coins within 14 days. As regards loot boxes, in 2022 the Commission sent a letter to two gaming organisations to remind them of the applicable consumer laws, in line with the updates to the UCPD Guidance. In May 2024, the Dutch authority fined Epic for unfair practices aimed at children in Fortnite, including direct exhortations to make purchases and misleading countdown timers to put pressure on them.

While the DSA strengthens the protection of minors on online platforms and social media in particular (e.g. requirement to take 'appropriate and proportionate measures' to protect minors and to conduct risk assessments), its scope extends to video games insofar as they qualify as an intermediary service or a platform.

Stakeholder views

Overall, there is currently **no EU legislation that specifically regulates addictive design or specific features such as virtual items or in-app currencies**. The DSA's Recitals 81 and 83 mention addictive design in the context of risk assessment of VLOPs and VLOSEs, e.g. referring to the „design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive

[248] For additional information, see Pieterjan Declerck and Nadia Feci (2022). 'Mapping and analysis of the current regulatory framework on gambling(-like) elements in video games – a report in the framework of the 'Gam(e)(a)ble' research project'.

behaviour“ and „online interface design that may stimulate behavioural addictions of recipients of the service“. The EP’s 2023 resolution on addictive design does not consider existing EU legislation, including the DSA or AI Act, to be sufficient. Concerning possible solutions to the identified problems, the consultations showed an increasing acknowledgement of the seriousness of the digital addiction problems, but views diverged on the appropriate measures to tackle them. Nevertheless, responses from academics noted that the empirical evidence that would enable to draw a link between the practices and their harmful effects is still emerging. Several stakeholders agreed that the **acceptable boundaries of addictive design** should be made clearer in the legal framework and through guidelines. Some traders highlighted the benefits of existing tools, such as parental controls, time limits and screentime monitoring, but expressed concerns about prescriptive legislation that would affect their freedom to design interfaces or product functionalities. In the public consultation, 51% of stakeholders supported mandating a functionality that allows consumers to **set limits to the amount of time and money** they spend using digital services. In the 2023 CCS, 27% of parents considered activating parental control tools to limit their children’s consumption but only 8% considered doing so for themselves. Similar ideas for control measures include receiving **notifications about time spent** after a specified daily time period. However, desk research and consultations suggest that such control tools are likely to be ineffective if not activated by default.

Several stakeholders called for mandating that traders **turn off by default addiction-inducing interface designs and functionalities**, while allowing consumers the option to turn them back on. For example, in 2023, TikTok established a default time limit of 60 minutes for users under 18 years old, which could be overridden through an active decision by entering their passcode.

In general, stakeholders representing children’s rights were not calling for preventing the access of children to specific services, but rather stressed the importance of ensuring age-appropriate design from the outset. The EP’s 2023 resolution on addictive design urged the Commission to further legislate on higher-risk features, including by **prohibiting the most harmful practices** and introducing a **‘right not to be disturbed’** that could turn all attention-seeking features off.

Furthermore, 49% of stakeholders in the public consultation called for more transparency about the **real price of virtual items** and 51% called for more information about the **probabilities of winning specific rewards from virtual items that have a randomisation element**. Aside from calls for transparency, some stakeholders consider the use of virtual in-app currencies *per se* as an unfair practice, especially for children, who have a more limited ability to calculate and to understand the real value of the transaction. It is notable that some of the difficulties with the estimation of the value of the virtual currency could be overcome if the currencies that can be bought with real money are kept separate from the currencies that can be earned in the game. In BEUC’s 2023 survey, 69% of consumers indicated that they would like more regulation around the sale of virtual items in games. Several stakeholders, including Member States such as NL and DK, called for a prohibition or stronger regulation of loot boxes and virtual in-app currencies. In 2022, 20 European consumer organisations, led by the Norwegian consumer organisation, called for more strict regulations for the gaming sector, such as mandating the display of prices in real currencies, prohibiting deceptive designs, prohibiting loot boxes and pay-to-win mechanisms in games likely to be accessed by minors, and clearer disclosure of when algorithmic decision-making is deployed to influencer consumer behaviour. The EP’s 2023 report on video games called for greater transparency, better enforcement of the existing

rules, ensuring that parental control tools and games directed towards children are consumer protective by design and by default, a common European approach to loot boxes, reducing addictive design features, introducing play modes without pay-to-win models and awareness-raising, among other measures. The EP considered that if the Fitness Check were to conclude that EU consumer law is not sufficiently protective, then the Commission should put forward a legislative proposal on these issues.

In 2024, France ordered a special commission of experts to draft a report on problems related to addictive design and the exposure of minors to screens. Their recommendations included a ban of the most harmful features and addiction-inducing features (e.g. infinite scrolling), developing European ethical standards, giving genuine choices to users, reversing the burden of proof regarding addictive design and algorithmic practices, restricting misleading, gambling-like or microtransaction-inducing practices in video games etc.

Taking the above into account, EU consumer law cannot be considered as sufficiently clear or effective in addressing the multifaceted harms resulting from interface designs and functionalities that induce digital addiction, which impairs consumer decision-making and puts vulnerable consumers, in particular minors, at a heightened risk.

VI.1.3. Personalisation (advertising, ranking, recommendations, pricing/offers)

Problems with personalisation

During the evaluation period, concerns about the **unfairness of B2C commercial personalisation** have increased, with recurring calls from consumer organisations to limit personalisation based on the tracking of consumer behaviour. The Commission's 2018 personalisation study, which included a survey of 23 050 consumers in the EU28 + Iceland and Norway, found that the main perceived benefits of personalisation include seeing more relevant products and discounts, a reduction of irrelevant ads and allowing for 'free' online services to exist, whereas the main concerns relate to the collection, use and sharing of personal data and the inability to opt-out/refuse.[249] The study also showed lower levels of awareness of personalisation among vulnerable consumers, such as older people, those with low educational levels, difficulties making ends meet, or less experience with online shopping.

The 2023 CCS found that 70% of consumers are concerned about how their personal data is used and shared, which amounts to a 21-percentage point increase compared to the same question about personalised advertising in the Commission's 2018 personalisation study. In the public consultation, **74% of consumers thought their personal data was misused or used unfairly** to personalise commercial offers in the preceding 12 months. Furthermore, the 2023 CCS found that consumers continue to be concerned about the processes concerning the collection of personal data and profiling (66%), installation of cookies (57%), negative effects on their trust in e-commerce (38%), seeing only a limited selection of ads and not the best offers (38%), inability to opt-out/refuse (37%) and inability to distinguish between information and advertising (35%). BEUC's 2023 survey found that **60% of consumers considered personal data analysis and monetisation to be unfair** and only 19% of consumers thought it is fair that they are targeted with

[249] The share of consumers who did not perceive any benefits ranged from 24% for ads, to 25% for ranking, and 32% for pricing.

personalised ads and content that is based on information about their lives and vulnerabilities.

The consumer survey conducted for this Fitness Check showed the following problems:

- 41% of consumers experienced a situation where the design or language of the website/app made it **difficult to understand how their personal data would be used**. This was particularly high for those consumers who consider themselves highly impulsive, and among those who find that spending time online negatively affects their daily lives, with 40% of these consumer groups respectively indicating that they regularly (or always) have this experience online. Furthermore, this was the most common issue indicated by the two oldest age groups (13% of those 55-64 and 12% of those 65+).
- 37% of consumers had the impression that the **company had knowledge about their vulnerabilities and used it for commercial purposes**. This was the most prominent issue among the youngest cohort (age 18-25), with 27% of respondents of this age experienced this 'always' or 'most of the time', and a further 24% experiencing this 'sometimes'.
- 34% of consumers stated they **did not have the option to opt-out** of personalised commercial offers (e.g. personalised prices or advertisements).
- 38% of consumers had **difficulties in understanding what kind of 'profile' the platform had created** based on their personal data and how it affected the content/information that was shown to them. This issue was particularly prevalent among those who are inclined to bet online (33% of those who bet online daily), as well as among those who feel spending time negatively affects their daily lives (42% who feel spending time online has very negative effects).
- 37% of consumers experienced **difficulties with changing their preferences** about how their personal data is used due to the design or language used on the website/app.

Whereas personalised advertising, ranking and recommendations are very widespread, evidence on personalised pricing is still emerging. The EP's 2022 study on personalised pricing analysed the different mechanisms and categories of price personalisation practices which can currently be observed on the market, and considered there to be a high likelihood that such practices will become more widespread in the near future. In general, consumers are unlikely to wish to pay a personalised price that is higher than the price offered to other consumers, unless it concerns second- or third-degree price personalisation (e.g. discounts for students) that is transparently communicated. First-degree price personalisation that exploits the consumer's willingness to pay to the benefit of the trader may be perceived as unfair by consumers, even if it is legally allowed. Moreover, price differences solely based on place of residence or location of the consumer that are not linked to differences in applicable taxes and/or services (including cross-border delivery) may, under certain circumstances, be prohibited under the Geo-blocking Regulation. The Commission's 2018 and 2022 studies[250] did not find consistent and systematic evidence of personalised pricing or offers. A sweep in the Fitness Check's supporting study identified price differences on 10 out of 85 websites/apps (in DE, IT, RO, SE, ES), without transparent indications regarding the reasons for price differences and whether personalisation was taking place. Additional research by consumer organisations has found evidence of price personalisation in the online dating, accommodation, and airline sectors.[251] Personalisation practices are

[250] 2018 personalisation study, 2022 dark patterns study
[251] BEUC (2023) Each Consumer A Separate Market? BEUC position paper on personalised pricing.

difficult to detect, even by experts and enforcement authorities (especially to re-trace the personalisation that was shown to a specific consumer). However, even though these price personalisation practices are not widely adopted yet, there is consensus among the stakeholders consulted for the Fitness Check that their prevalence will increase in the coming years with advancements in AI, making them more accessible to traders of different sizes.

Legal framework

Despite the concerns that consumers expressed about profiling and data use, B2C personalisation practices are not *per se* unfair or illegal according to the Directives under evaluation, provided that the trader has fully complied with the GDPR, ePrivacy Directive, DSA, DMA and other applicable legislation, such as the AVMSD[252]. Possible legal concerns arise from the consumer protection perspective if traders are **not sufficiently transparent about the personalisation or if they make use of information about the vulnerabilities of specific consumers or a group of consumers** to distort their decision-making in a commercial context. Such practices have also been detected in the offline environment, e.g. with relatives of a deceased person receiving letters about gravestone advertisements, but the opportunities for wide-spread vulnerability exploitations are much larger in the online environment. Risks can also increase as the data about the behaviour of one consumer could affect other consumers that share similar characteristics if traders draw inferences and adapt their commercial practices based on those assumptions. Furthermore, such assumptions could be fed into algorithms and AI systems that are subsequently used for non-commercial and possibly sensitive purposes. Mystery shoppers in the Commission's 2022 dark patterns study were not able to identify significant cases of vulnerability exploitations in personalised advertising, prices, ranking and recommendations. However, the consultations and data collection found several relevant examples, such as the 2023 report by the Swedish authority which showed that indebted consumers regularly received targeted offers for new consumer credit in a manner which implied that it would improve their financial situation. Notably, the recent amendments to the CCD provide that Member States shall prohibit advertising for credit products which encourages consumers to seek credit by suggesting that the credit would improve their financial situation (Art. 8(7)(a)).

Additional examples of potentially manipulative or opaque personalisation were highlighted in the sweep of the Fitness Check's supporting study, covering 53 dating and gambling websites/apps in 10 Member States and 3 global sites. The sweep provides anecdotal evidence of the types of practices that consumer can encounter. The sweep involved preparatory activities to create indications that the consumer may be experiencing vulnerabilities related to financial distress, low morale/depression and family issues (social media usage and web searches, e.g. 'how to deal with grieving'). None of the gambling websites/apps displayed advertisements referring to external products or services, only internal promotions. In the case of dating websites/apps, researchers considered that 42% of the ads appeared to be linked to vulnerabilities, including in some cases linked **to the previously indicated vulnerabilities**, although it was not technically possible to conclude whether there was a direct connection. For example, ads about taking out loans or romantic encounters appeared after making searches related to relationship and money problems. None of the traders provided an explanation of personalised advertising or recommendations upfront, but in the majority of cases, consumers were given basic information in T&Cs/privacy policies that personalisation practices were used (88%

[252] See Articles 6a(2) and 26b(3) on prohibitions of using personal data of minors for commercial purposes.

mentioned personalised recommendations, 78% personalised ads and offers), without any specific information about how the personalisation is performed or the criteria used. None of the traders gave an option to turn off personalisation practices.

Case law and enforcement activities using the three Directives in relation to personalisation practices have been limited. However, a number of consumer authorities in the CPC network have started to share best practices on how to apply consumer law to personalisation practices and engage in dialogue with data protection authorities. In 2022, this cooperation resulted in a non-binding document outlining '5 key principles of fair advertising to children'.

The 2022 CPC action against TikTok, led by the Irish and Swedish authorities, resulted in commitments that made the use of personalised advertising more transparent, including by adapting ads policies, redesigning the personalised ads permissions prompt for EEA consumers and by implementing a reporting category for ads that could contain direct exhortations to children.

Concerning personalised pricing, the 2022 CPC coordinated action against Wish.com, led by the Dutch authority, uncovered that it had not been clear whether and how the trader applied price personalisation. The regulatory dialogue led to Wish taking the decision to stop their personalised pricing techniques in the EU as of 25 May 2022. The 2024 CPC coordinated action against Tinder resulted in commitments to: not apply personalised pricing based on age without informing consumers clearly and upfront about it; informing consumers clearly that discounts on prices for premium services are personalised using automated means and; and informing consumers why they are offered personalised discounts, for example because they were not willing to purchase Tinder's premium services at a standard rate.

Concerning coherence with new legislative developments, the evaluation period included the entry into application of the GDPR, which established comprehensive rules for all processing of personal data by controllers and processors established in the EU and outside the EU that offer services or goods to individuals in the EU or monitor their behaviour in the EU. Manipulative or opaque personalisation practices could entail a breach of several GDPR provisions, such as the principles of fairness and transparency. The Fitness Check did not identify major coherence concerns between the GDPR and the three Directives. However, several stakeholders called for more clarity on the interpretation of certain GDPR provisions which interplay with consumer law, such as the applicability of Article 22 GDPR to price personalisation.

Regarding personalised pricing, the Modernisation Directive introduced in the CRD a mandatory obligation for traders to disclose the presence of personalised pricing. This provision has established a minimum level of transparency about personalisation at the point of sale, complementing the GDPR. However, the provision does not require **any further explanation about personalised pricing at the point of sale, such as the data or main parameters used in its determination**. To the extent it constitutes automated decision-making with legal or similarly significant effects, additional explanations can be provided under Articles 13 and 14 GDPR. The provision also does not address any other aspects of personalised pricing beyond transparency, such as risks concerning the limitation of access to products and services for certain consumers. Several stakeholders considered this information obligation to be ineffective. The Commission's 2018 personalisation study and the OECD's 2021 report on personalised pricing, which both

included a behavioural experiment, found that such transparency disclosures had limited effects on the consumer's shopping behaviour.

In the area of consumer financial services, the amended CCD provides that Member States shall require that creditors and credit intermediaries 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 (Art. 13).

Recent examples of national laws in this area include a 2023 Italian law concerning airline ticket pricing, which included restrictions to the use of automated pricing algorithms based on user profiling where this would 'adversely affect the economic behaviour of the user'.

Regarding personalised ranking and product recommendations, the Modernisation Directive introduced in the UCPD and CRD an obligation for traders that provide the consumers with the possibility to search for other traders' products, i.e. online marketplaces and price comparison sites, to provide consumers with general information about the main parameters determining ranking of offers as a result of the consumer's search query and the relative importance of those parameters as opposed to other parameters. The scope of this provision does not cover **traders that provide consumers with a possibility to search only amongst their own offers of different products.** It also does not cover the **ranking within the default organisation of the online interface that is not the result of a specific search query**. Moreover, the transparency obligation does not extend to online search engines, as those were already covered by a similar obligation in the Platform to Business Regulation that was adopted earlier.

In case of any recommender system provided by platforms, moreover, the DSA mandated more transparency in the T&Cs about the main parameters used as well as information and functionalities regarding options for consumers to modify or influence those parameters. In case of VLOPs and VLOSEs, the DSA mandates at least one recommender system option not based on profiling. Concerns related to personalisation could also be tackled through the risk assessments and mitigating measures that the DSA requires from very large players.

Regarding personalised advertising, the DSA strengthened the required level of transparency towards consumers and established an obligation not to present personalised advertising based on profiling using special categories of personal data under the GDPR and towards minors. The scope of these DSA provisions covers online platforms, which excludes other types of traders that may engage in personalised advertising. Furthermore, the prohibition regarding sensitive data is limited to the special categories of personal data referred to in Art. 9(1) GDPR (i.e. data related to race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, health, sex life and sexual orientation). Special categories of personal data are any data, including an output from another data that reveal any of the categories listed in Article 9(1) GDPR. The CJEU interprets 'sensitive data' broadly but the case law at this stage does not resolve whether that covers all **types of vulnerabilities flagged in the Fitness Check, including consumer data that could be broadly considered as sensitive in the B2C context**, e.g. data regarding behaviours or mental states such as emotions, moods or thoughts, or data regarding negative events such as relationship problems, death of a family member, financial challenges or gambling problems.

The DMA restricts, under specific conditions, the ability of gatekeepers to combine and cross-use consumers' personal data from a core platform service with data from other services provided by the gatekeeper or third parties. Gatekeepers also have to enable end users to freely choose to opt-in to certain data processing and automatic sign-in practices by offering a 'less personalised but equivalent alternative', and without making the use of the core platform service or certain functionalities thereof conditional upon the end user's consent. The less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent. In effect, this provides consumers with a right to a less personalised commercial offer for certain digital services.

Concerning personalisation more generally, the AI Act prohibited specific use cases 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, which leads or is (reasonably) likely to lead to significant harm. The application of these prohibitions is dependent on the interpretation of specific terms (such as 'subliminal technique' and 'purposefully manipulative or deceptive'), the resulting harm must be considered as significant and not all types of vulnerabilities are covered. Furthermore, when updating the list of high risk AI systems, one of the factors that should be taken into account is the extent to which there is 'an imbalance of power, or the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age'. The AI Act clarifies that personalised advertising that complies with the applicable law should not be regarded as harmful or manipulative *per se*. Furthermore, it is not necessary to prove that the trader had the intention to cause significant harm. The AI Act suggests that practices falling outside of the scope of these prohibitions could be covered by the existing data protection, consumer protection (in particular as regards the UCPD, the prohibitions in the AI Act are considered complementary) and digital services legislation.

Other relevant legislation with a narrower material scope includes the AVMSD, which prohibits the use of subliminal techniques in audiovisual commercial communications provided by media service providers and video-sharing platforms, thereby limiting the exploitations of such vulnerabilities through television, on-demand audiovisual media services, and certain types of online services.

Beyond legislation, in 2023-2024 the Commission facilitated stakeholder dialogue towards a **Cookie Pledge** consisting of voluntary pledging principles regarding cookies and other similar technologies capable of tracking users' online navigation. The overall objective was to counter 'cookie fatigue' and empower consumers to make more effective choices regarding tracking-based advertising models. The discussed pledging principles can be summarised as follows:

- no information on cookie banners about cookies that do not require consent;
- inform consumers upfront when content is at least partly financed by advertising;
- explain the business model and the consequences of accepting or not-accepting trackers in a clear manner;
- provide consumers with a choice between tracking-based advertising and a less intrusive model, such as contextual advertising or advertising based on topics selected by consumers;
- do not give the impression that consent must be given for every single tracker;

- no separate consent for cookies strictly necessary for the delivery of the advertising model selected by the consumer;
- respect and store consumers' choice to refuse cookies for a year;
- explore solutions to record consumers' cookie preferences, including a positive preference to accept certain types of advertising.

However, the Cookie Pledge was a voluntary initiative and did not conclude with commitments or signatures from market players in 2024.

Stakeholder views

Feedback to the public consultation highlighted disagreement on whether personalisation practices benefit consumers and whether the current framework is sufficient. Many traders and business organisations argued in favour of the status quo, while several other stakeholders such as consumer organisations and enforcement authorities pleaded for introducing more fairness and **consumer choice**. For certain traders, the ability to rely on personalised advertising is reported as absolutely essential and any restrictions are considered to produce significant negative impact.

However, the reliance on personalisation may vary per trader size, as shown by the business survey, which mainly included SME-s, and where 76% of traders indicated that they had not collected personal data from consumers. Those that used consumer data applied it to help decide which offers to feature more prominently (31%), how to tailor or customise advertisements (30%) or to tailor the price of their products/offers (18%).

Another difference of incentives concerns the personalisation practices deployed by traders whose business model relies on monetising consumer data and those that rely primarily on subscriptions. Several stakeholders and national authorities acknowledge a middle ground, where **the freedom to use personalisation should exist up to the point where the commercial practices become intrusive or exploit vulnerabilities**.

While there was consensus that the exploitation of consumer vulnerabilities for commercial purposes is problematic (79% of respondents to the targeted survey agreed or strongly agreed with this assertion), views diverged on whether more regulation is necessary. Several stakeholders considered that the three Directives **do not provide sufficient certainty on the legal boundaries of acceptable commercial personalisation**, which creates difficulties for compliance and enforcement. In particular consumer organisations and certain Member States, questioned the justification for the narrowing of some of the new prohibitions of unfair personalisation only to online platforms, thereby leaving out other traders and digital services that may also have a significant influence on consumer behaviour. For example, they called for **establishing equivalent obligations in EU consumer law that would be applicable to all traders, such as the DSA's prohibition of presenting targeted advertising towards minors or based on sensitive data**. Similarly, the personalisation-related prohibitions in the AI Act may not cover all types of vulnerabilities or manipulative techniques that pose risks in the B2C commercial context. Emotion-recognition AI (high risk but not prohibited under the AI Act) and anthropomorphic AI that emulates human behaviour and emotions were flagged as major concerns.

Several stakeholders were critical of the efficacy of transparency obligations in this area and called for clearer prohibitions of unfair practices, such as adding to the UCPD **blacklist commercial practices using psychographic profiling** or similar techniques that create pressure and exploit personal vulnerabilities, including temporary vulnerabilities such as emotional distress, exhaustion, grief, sorrow, physical pain, influence of medication. Furthermore, 48% of stakeholders in the public consultation supported the introduction of

a more **explicit option to receive non-personalised commercial offers** instead of personalised ones.

Furthermore, BEUC's 2023 survey found that 75% of consumers thought **children need more protection** from behavioural monitoring and influencing, even after the introduction of new protective measures in the DSA. Similar opinions were expressed by several national authorities who do not see the current framework as sufficiently taking into account the vulnerabilities of young consumers and the concerns regarding the use of their data.

The EP's 2022 study on personalised pricing offered several recommendations for targeted prohibitions: a) prohibition of personalised price increases, while allowing personalised discounts and other price differentiations that are transparent and justified; b) prohibitions related to certain industries, namely for universal services; c) prohibitions related to certain criteria (beyond anti-discrimination law), such as the exploitation of vulnerabilities (e.g. sensitive data, medical conditions, anxiety, addiction). In cases where price personalisation is allowed, information obligations could be further reinforced by requiring 'meaningful information about the logic involved' in a way that consumers can understand, and by improving the placement of the CRD price personalisation disclosure (e.g. requiring it to be displayed right next to the price) as well as its scope, which could be extended to additional sectors outside of the CRD scope and to offline scenarios (e.g. electronic price labels in shops).

BEUC has called for the **prohibition of personalised pricing based on behavioural predictions**, such as assessing the willingness to pay, unless it is third-degree price personalisation (i.e. differentiation based on verifiable demographic characteristics such as age) or it is fully transparent and limited to data and types of assessment that are strictly necessary for performing a service (e.g. insurance risk assessments). Trade organisations noted that any considerations towards prohibitions of personalisation practices should include appropriate exemptions for specific use cases, e.g. in case a specific product/service is inherently personalised.

Several stakeholders gave B2C personalisation as a prime example of a type of commercial practice that is technologically complex and where consumers and authorities face undue difficulties in proving an infringement, thereby necessitating an alleviation of the **burden of proof**.

Taking the above into account, in its current form, EU consumer law cannot be considered sufficiently effective or clear in addressing the multifaceted concerns regarding commercial personalisation. An effective response would require further assessment under both consumer protection and data protection frameworks.

VI.1.4. Social media commerce and influencer marketing

Problems with commercial practices on social media platforms

Given the increasing importance of social media for consumer transactions, the Fitness Check evaluated problematic practices concerning the advertising or direct selling of products to consumers through social media, including influencer marketing. According to Eurostat, in 2021 more than half of traders (59%) reported using at least one type of social media, which is a 22 percentage point increase compared to 2015. BEUC's 2023 survey found that 73% of consumers have encountered promotions by influencers and 53% report

buying products or services recommended by them.[253] Other research at national level shows similar tendencies among French, Italian, Irish, Belgian and German consumers.[254]

Direct purchasing possibilities through social media platforms (e.g. 'buy' buttons, shopping carts) have not yet been widely rolled out in European markets, but consumers can already discover, research and buy products through a redirection to the seller's website, without leaving the app environment. Different trends and business models continue to evolve (e.g. **livestream shopping**) and social media platforms are well placed to make use of IoT and augmented or virtual realities.

As shown by numerous studies and enforcement activities, a common concern with social media advertising and influencer marketing in particular is the **non-compliance** with the requirement in the UCPD (in addition to the AVMSD, e-Commerce Directive and DSA) to clearly **disclose commercial communications**. In the public consultation, 74% of consumers reported **a lack of transparency** about the paid promotions of products by social media influencers and 55% of respondents reported the same in the 2023 CCS. In the consumer survey for this Fitness Check, 45% consumers noticed that the content they were viewing seemed to be a paid promotion or advertisement, but the website or app did not make this clear. This was **particularly high amongst those in the younger age groups** (28% of 18-25 year-olds, and 29% of 26-35 year-olds, compared to 11% of 55-64 year olds, and 10% of those aged 65+).

A 2021 study conducted by the Danish authority found that both children (38%) and adults (56%) have difficulties with distinguishing between commercial and non-commercial content. The study also showed that more prominent, visually salient and standardised disclosure labels can help improve recognition, but a significant share of consumers would still fail to notice or understand that they are seeing commercial content. A 2021 study by the Dutch authority and a 2022 study by the Danish authority focusing on paid ranking in search results showed that consumer understanding of disclosures is generally low and that effective disclosure requires a necessary degree of prominence, proximity and intuitiveness (i.e. ease to understand without the need for further explanations). The OECD's 2022 report on online disclosures provides further insights into existing research and the key challenges that remain.

Compared to other forms of online advertising, influencer marketing has even fewer characteristics that make it possible for consumers to detect the commercial nature of the content. Even if an influencer uses disclaimers, consumers could assume that the content is presented at least partly as a personal recommendation rather than a clearly identifiable direct advertisement. The 2022 EP study on influencer marketing described the various practices that may pose risks for consumers.

Concerns arise not only with hidden marketing, but also with the possibly **problematic content of the advertising**, such as specific products or services promoted or sold through influencers. BEUC's 2023 survey found that 44% of consumers have seen influencers promoting scams or dangerous products. The exposure of children to aggressive marketing of unhealthy food and beverages, alcohol or vaping, is also a point of increasing concern. BEUC's 2021 survey also shows a strong influence of such marketing on children's behaviour and that children are targeted by unhealthy food and beverage ads. According to the recent scientific opinion "Towards Sustainable Food consumption" prepared by Scientific Advice Mechanism (SAM), advertising unhealthy diets and foods that are poor

[253] BEUC (2023) From influence to responsibility, Time to regulate influencer marketing.
[254] Ibid., p. 5.

in nutrients or high in fat, salt and sugar to children should be banned in all media. The SAM opinion shows that voluntary codes of conduct for responsible marketing are not sufficient to address the issue.

Several Member States, including by making use of the AVMSD rules applicable to influencers, have adopted or updated laws (FR, ES, IT, NL, DK) and guidelines that contain definitions and specific obligations for influencers and traders that work with them. The 2023 French law introduced, among other issues, prohibitions of influencer marketing involving plastic surgery/injections, pharmaceutical products and medical devices, nicotine, certain financial investments (e.g. crypto) and wild animals; gambling and sports betting/prognoses are allowed subject to limitations of access to minors. Other examples of relevant national legislation include the 2022 changes to German law that created a presumption of remuneration for the commercial communication, unless the influencer proves otherwise.[255]

Legal framework

EU consumer law does not explicitly address 'social media commerce', but the existing rules concerning pre-contractual information, marketing and contract terms apply to social media platforms when they act as online marketplace. For example, platforms that enable the direct purchasing of products during livestream shopping should ensure that it is technically possible for influencers or sellers to comply with EU consumer law requirements. The transactional journey for purchases made through in-app browsers should be clear for consumers, although there are currently no specific information obligations in the Directives that expressly mention this scenario.

With regards to influencer marketing, the UCPD can be and is already used to tackle several problematic practices, such as the lack of disclosure of commercial communications, false or misleading marketing claims (e.g. exaggerated claims about health products or financial services) or direct exhortations to children. Furthermore, following amendments by the Modernisation Directive, the purchasing of fake likes and followers is a prohibited practice in point 22 of the UCPD blacklist. When influencers act as direct sellers of products or services, all of the applicable consumer laws would apply.

In 2021, the Commission provided additional clarifications in the UCPD Guidance about aspects such as the qualification of influencers as 'traders' or 'agents acting on behalf of a trader' (regardless of the size of their following), the interpretation of the concepts of 'editorial content' (to include social media content), 'payment' (to include any form of consideration with an asset value, in line with the case C-371/20 Peek & Cloppenburg), guidance on a sufficiently salient disclosure (e.g. need to individually label each commercial communication; no vague hashtags at the end of lengthy disclaimers; no requirement for the consumer to take additional steps to see the disclosure) and an acknowledgement that the breach could be attributed to both the influencer and the brand, regardless of the presence of editorial control by the latter.

However, given the non-binding nature of the guidelines and in the absence of CJEU case law confirming the interpretation and without specific provision in the UCPD , there remains **legal uncertainty about the applicable rules, including about the responsibilities of other actors in the value chain, such as the brands whose products and services are being promoted (besides that of platforms, regulated *inter alia* in the DSA)**. Furthermore, aside from the limitations established in the AVMSD for audiovisual

[255] § 5a para. 4 Unfair Competition Act.

commercial communications and other sector-specific legislation, there are no specific prohibitions preventing influencers from advertising certain products, which risks regulatory fragmentation.

Case law and enforcement activities in the area of social media ads and influencer marketing have increased during the evaluation period. However, actions regarding other aspects of social media commerce, such as selling to consumers, remain limited, which is partly the result of the limited roll-out of such features thus far.

The existence of an EU-wide obligation to disclose commercial communications has enabled several national courts and CPC authorities to tackle the lack of transparency with influencer marketing. For example, the Belgian authority has launched over 90 investigations into influencer marketing. Concrete examples of recent actions include the 2023 investigations by the French authority after finding that 60% of influencers did not comply with clear disclosures. In 2023, the Polish authority took action against both the influencers and the trader working with them, highlighting in particular the active role that the trader played in directing the influencers to disregard clear disclosures. In 2023, the Italian authority fined an influencer and the brands working with her due to misleading information suggesting that a purchase of the advertised product would contribute to a hospital donation made by those brands. The 2021-2022 CPC coordinated action against TikTok and the 2021-2023 action against Google also involved concerns about the lack of clear ad disclosures. In order to ensure an evidence-based response, the Commission also undertook behavioural experiments to test the efficacy of specific ad labels in the proposed commitments in these actions. The 2022 EP study on influencers gives several additional examples of cases of influencers advertising harmful or illegal products, such as pyramid schemes. In 2023, BEUC issued an external alert to the CPC network concerning misleading promotions of crypto products on social media, including by influencers. The alert requested that social media platforms prohibit influencers from promoting crypto products.

In 2024, the results of a sweep carried out in accordance with the CPC Regulation of social media posts from 576 influencers[256] found that while nearly all of the influencers posted commercial content, just 20% systematically indicated the commercial nature of the content shared. Furthermore, 38% did not use the platform-facilitated tools to disclose the commercial nature (e.g. 'paid partnership' toggle on Instagram). There was divergence in the wording used in the disclosures, such as 'collaboration (16%), 'partnership' (15%) or generic gratitude expressed for the brand (11%). Just 40% of the influencers made the disclosure immediately visible during the commercial communication, while 34% opted for less visible disclosures that required the consumer to take additional steps, such as click on 'read more' or scroll down. Overall, despite the presence of long-standing clauses in the UCPD concerning hidden advertising, widespread non-compliance shows the limits of the current regulatory framework. It is also notable that 40% of influencers were endorsing their own products, services or brands, which shows that they are increasingly taking on

[256] Of the 576 influencers that were checked, 564 where nationals of the EU, Iceland or Norway. Several influencers were active on different social media platforms: 572 had posts on Instagram, 334 on TikTok, 224 on YouTube, 202 on Facebook, 82 on X (former Twitter), 52 on Snapchat, and 28 on Twitch. The main sectors of activity concerned, in decreasing order, fashion, lifestyle, beauty, food, travel and fitness/sport. 119 influencers were considered as promoting unhealthy or hazardous activities, such as junk food, alcoholic beverages, gambling, or financial services such as crypto trading, or activities that can involve risks and need to be exercised by qualified professionals such as medical or aesthetic treatments. 82 influencers had over 1 million followers, 301 over 100,000 and 73 between 5,000 and 100,000.

the role of traders and sellers, not merely facilitating marketing. 44% of influencers had their own websites and most of these included selling to consumers.

Next to enforcement activities, several authorities, self-regulatory bodies[257] and the industry itself have contributed to awareness-raising about the applicable rules in this area. In 2023, the Commission developed the Influencer Legal Hub, which aims to provide influencers, advertisers, agencies and brands with basic guidance on how to comply with EU consumer law as described above. It also provides recommendations such as strongly advising influencers to regularly check the Safety Gate Portal to ensure that the product they advertise were not notified as unsafe.

However, despite these efforts and the presence of an EU-wide legal transparency obligation, there remains considerable **legal uncertainty about the required standard and modalities of ad disclosures**. Different courts, authorities, national laws and guidelines offer different interpretations about aspects such as the exact phrase to be used and the necessary visual prominence. For example, although the UCPD Guidance states that full transparency is required also in case the influencer is promoting their own products or services, the German Federal Court of Justice ruled that the commercial intent is more apparent in such cases and disclosures can therefore be more limited.[258]

Concerning coherence with new legislative developments, the DSA, while confirming the conditional liability exemption about the content hosted by platforms (including whether the influencer is complying with rules on commercial communications), introduced a general obligation for platforms to provide recipients of the service with a functionality to declare whether the content they provide is or contains commercial communications, triggering a clear and prominent marking allowing to identify the commercial nature of the content (Article 26(2)). In addition to that, obligations aimed at 'online platforms that allow consumers to directly conclude distance contracts' could be applicable to social media platforms that enable such functionalities. Moreover, platforms that allow consumers to directly conclude distance contract shall ensure that the rules on the traceability of traders (Article 30) are also applicable to any traders promoting messages through the use of their platform. The DSA also strengthens online advertising transparency more generally, for example by requiring larger players to create online ad repositories that enable consumers to better understand why they were shown specific ads.

The DSA also foresees an obligation for the Commission to promote inter alia the **standardisation of ad disclosures, which could alleviate existing uncertainties and facilitate a common European approach**. It should be noted that the general provisions concerning advertising do not cover all instances of influencer marketing, as the DSA only covers 'advertisement' as a service, in other words, on the basis of remuneration to be given to an online platform. However, influencers are in any case covered by the references to 'commercial communications' in the DSA. In addition, in cases where the influencer's content amounts to illegal content by breaching EU laws (e.g. by promoting medicines that require a prescription[259]), the DSA significantly facilitates the reporting and removal of

[257] For example, the European Advertising Standards Alliance's Influencer Marketing Standard Training (IMST) explains to influencers, in their own language, how to behave responsibly when promoting products or services, with particular emphasis on disclosure obligations. An "influencer certificate" will come as a second step, building on EASA network's data-driven ad monitoring capabilities. Further information is available under https://www.easa-alliance.org/responsible-influence/

[258] Judgment of 9 September 2021, court case no. I ZR 125/20.

[259] Contrary to Article 9(1)(f) of Directive (EU) 2018/1808 (the revised AVMSD) and Art. 88(1)(a) of Directive 2001(83(EC on medicinal products for human use.

such content, but it did not introduce any new prohibitions concerning specific content that can be shared by influencers.

The AVMSD's 2018 revision clarified the scope of the existing rules and provided additional rules for media service providers and video-sharing platforms, such as the need to disclose commercial communications, prohibiting certain types of ad content (advertising tobacco products, electronic cigarettes, medicinal products/treatments available on prescription in the Member State within whose jurisdiction the media service provider falls, advertising alcohol to minors, encouraging behaviour prejudicial to health or safety), requiring measures to protect minors from harmful content, mandating a functionality for users who upload user-generated videos to be able to declare whether it contains commercial communications and requiring Member States to encourage co-regulation and self-regulation as regards the advertising of unhealthy food to minors. These rules can apply directly to influencers when they fulfil certain criteria (e.g. they engage in a significant economic activity, have editorial control on the content they provide, have the general public as target audience) and thus can qualify as providers of audiovisual media services. In this respect, the European Regulators Group for Audiovisual Media Services (ERGA) has provided guidance on the application of the AVMSD rules to influencers. In particular, the specific requirements related to advertising transparency, advertising fairness, and protection of vulnerable groups (in particular minors) can apply both in the scenario where an influencer could be considered as a provider of audiovisual media services and in the scenario where an influencer is a user of a video-sharing platform service, but does not fulfil the relevant criteria to qualify as audiovisual media service provider. Therefore, the AVMSD remains the main EU legislation regulating specific content requirements for influencers' audiovisual commercial communications and complements EU consumer law on influencers marketing practices. It is important that full complementarity and alignment are ensured between EU consumer law initiatives and new content requirements for influencers that may be introduced in the AVMSD during the ex-post evaluation of the Directive, which is meant to take place by 19 December 2026[260].

In the area of financial services, in 2023 the Commission proposed a revision of the retail investor protection rules, which included new transparency and fairness requirements for marketing communication and practices, covering also promotions through social media influencers and recognising the relevance of non-monetary compensation. Furthermore, under the proposed rules, the investment firm whose products were promoted would have to keep records of all marketing communications for several years.

While the existence of different EU laws applicable to influencer marketing is not indicative of incoherence as such, it raises risks in the implementation stage. Case law, enforcement actions, guidelines, codes of conduct and other activities related to these legislative instruments could lead to diverging interpretations concerning the same set of commercial practices, such as establishing different standards for ad disclosures or prescribing different requirements for influencers based on the size of their following. For example, the Dutch media authority required registration only from influencers that have more than 500 000 followers in the context of the AVMSD application, whereas no such thresholds exist under the UCPD.

Stakeholder views

[260] Article 33 of Directive (EU) 2018/1808 (the revised AVMSD).

Concerning possible solutions to the identified problems, 58% of stakeholders in the public consultation were in favour of further **clarifying the concept of an influencer/content creator** and the **obligations that the various traders involved with influencer marketing have towards consumers** (e.g. influencers, agencies, brands, platforms). Concerning the definition of influencers, a submission from a group of academics proposed three options for potential action: the adoption of a concept of 'influencers' or 'prosumers' or expanding of the existing definition of traders, with preference for the latter as the least disruptive measure. Some stakeholders call for **holding agencies and brands liable for monitoring the compliance by influencers with EU laws**, which would increase incentives for partnering with more compliant influencers, giving clearer instructions, and including contractual clauses to this effect. It was also suggested that several legal interpretations from the Commission's UCPD Guidance could be codified into law for increased legal certainty.

While there was broad acknowledgement, especially by business organisations, that the UCPD can cover several types of commercial practices, there is a **considerable risk of regulatory fragmentation** in this area without EU intervention. Concerning ad disclosures, instead of reconciling tens of diverging national court decisions and guidelines, it can be more efficient to **prescribe examples of accepted labels at EU level**, whether through standardisation in the DSA context (limited to online intermediaries like social media platforms) or more generally in EU consumer law for all traders.

Concerning harmful content, BEUC calls for the prohibition of influencer marketing in areas similar to those listed in the French influencer law, highlighting in particular the promotion of alcohol, gambling and sports betting/prognoses, medical products/procedures and unhealthy food to children.

The EESC, in its 2023 exploratory opinion on influencers, while recognising that the existing EU legal framework provides adequate protection, called for a more harmonised treatment of influencer marketing at EU level, including the introduction of specific legislation on influencers and a joint and several liability of platforms for illegal content published by influencers. It also called for ensuring the technical possibility of preventing underage users of platforms from viewing sensitive content (e.g. alcohol and energy drinks, gambling and betting activities, pornography, tobacco and tobacco products, including e-cigarettes, aesthetic surgery etc.). BEUC's 2023 survey found that 74% of consumers consider that platforms should be held more responsible for the content that influencers post.

In May 2024, the Council adopted Conclusions on support for influencers as online content creators, covering both B2C advertising aspects and broader impacts. The Council called on the Commission to reflect on a coherent approach to influencers across all policy areas, with a focus on responsible behaviour. Various measures were proposed to ensure that influencers have better knowledge and media literacy skills, including by updating the Commission's Influencer Legal Hub.

In conclusion, while EU consumer law establishes a general legal basis for tackling transparency concerns regarding influencer marketing, it is currently insufficiently precise in addressing all concerns raised by social media commerce, which contributes to a risk of regulatory fragmentation and legal uncertainty.

VI.1.5. Contract cancellations and digital subscriptions

Problems with digital contracts and subscriptions

Given the exponential growth of the digital subscription economy and the trend towards 'freemium' business models, the Fitness Check examined some of the commonly reported problems consumers face when concluding contracts online, such as difficulties with the online cancellation of contracts, automatic renewals of subscriptions, free trials, subscription price hikes and contract duration. Specific concerns with unfair contract terms are tackled in a separate section.

51% of consumers responding to the consumer survey indicated that they had purchased, used, renewed, or cancelled a digital subscription in the preceding 12 months. Younger consumers were more likely to have subscriptions (74% of those aged 18-25, and 71% of those aged 26-35) in comparison to older age groups (29% of those aged 56-65 and 31% of those aged 65+). Subscriptions were also more popular among consumers in the higher income deciles - 63% of consumers on average had used these services in the top three deciles vs 43% in the bottom three. Further, subscriptions were used most frequently by consumers who have indicated that they are trusting of online businesses and websites (75%). On a country level, subscription services were most popular in Spain (63%) and least popular in Hungary (37%). One in three consumers (33%) surveyed also indicated they had activated a free trial in the preceding 12 months, with younger consumers being more likely to have done so (54% of 18-25 year-olds and 51% 26-35).

In the public consultation, 69% of consumers found it **technically difficult to cancel their contracts**, 55% experienced **deliberate avoidance** of contract cancellation by the trader and 34% were only able to cancel their subscriptions after a longer time period (e.g. a year), despite being charged monthly. Furthermore, in the 2023 CCS, 23% of consumers reported difficulties with cancelling a contract that they had concluded online. In the consumer survey, 40% considered that the **design of the website/app made cancelling the subscription very difficult** and 42% experienced situations where the cancellation of the digital subscription was only possible after a long period. Furthermore, 54% of consumers had experienced a situation where the design and/or language of the website made it **unclear if the cancellation of their contract was successful** (e.g. no confirmation of termination appeared on the screen or was sent via email). As highlighted in the context of dark patterns, if traders add 'friction' into interface design (i.e. requiring more clicks, slower load time, text rather than image, need for active input like writing), it becomes more difficult for consumers to exercise their rights, such as their right to contract cancellation.

However, there may also be other reasons why cancellations become difficult. Traders that responded to the business survey said that, within the prior 12 months, 13% had refused to cancel a subscription contract after a customer requested it. Of those that had refused, 48% did so because the contract terms specified that the contract can be cancelled only at the end of the contractual period or after a certain time period has passed, or they were in a situation where the consumer had allegedly been in breach of contract (32%) or the consumer claimed the contract terms were unfair, but the trader disagreed with that assessment (20%). The supporting study for the Fitness Check found there to be challenges in cancelling a variety of services in different sectors such as software, travel insurance, digital media, such as online newspapers and the provision of maintenance services, such as for gas boilers.

Concerning the renewal of contracts, 62% of consumers in the public consultation experienced **automatic renewals of inactive subscriptions without reminders**. Auto-renewals can be convenient and beneficial for consumers, but the consumer survey showed that they also cause problems for consumers. Thus, 44% consumers reported that, after the initial contract period had expired, their digital subscription got automatically renewed and they had to pay again even though they did not intend to extend the subscription. Consumers also indicated that they continued paying for a digital subscription that they had stopped using some time ago but forgot to cancel (18% encountered this often, 19% sometimes).

Renewals can also involve heavily discounted initial promotional prices, followed by significant **price increase** later on (so-called 'loyalty traps' when price increases are applied to existing customers). In the consumer survey, 40% consumers had experienced an unexpected price increase of the subscription after the end of the initial promotional or free subscription period (e.g. it had not been clear that the price they were paying was a promotional price). More generally, in the sweep, the cost of the subscription was clearly presented in just 61.7% of cases, despite being a clear requirement under the CRD and UCPD.

Furthermore, **free trials** could convert into paid subscriptions with only passive consent from the consumer or without adequate pre-contractual information making it clear that the consumer is entering into a paid contract unless they cancel before the free trial period ends. The Commission's 2016 study on subscription traps, which covered 900 websites/apps in the areas of cosmetics and healthcare products, food and health supplements, dating services and digital services (i.e. cloud-based backup and video/music streaming services), found unclear information on charges (40%), missing or poor information on the duration of the trial (41%) and the subscription (45%), and on how and when the consumer can withdraw or unsubscribe (43%). The 2023 CPC sweep identified 'hidden information' as the most common dark pattern and in several cases such misleading practices had the aim of manipulating consumers to enter into subscriptions. The Commission's 2020 survey on scams and fraud found that 8% of respondents had fallen victim to a subscription trap and the estimated financial cost relating to online subscriptions was approximately 1.92 billion EUR across a two-year period.

In the consumer survey, 29% of consumers reported often having their **free trial automatically converted into a paid subscription**, without them being aware this would happen, while a further 21% indicated that this happens sometimes whilst 24% never experienced this. In the sweep, all of the examined subscriptions would be automatically turned into paid subscriptions if no action was taken by the consumer by the end of the trial. Just 16% of consumers in the consumer survey indicated that, after the end of the free trial period, they were always asked to explicitly agree to a paid subscription if they wanted to continue the service, whereas 20% indicated this happens most of the time and 21% sometimes. For many consumers, it was **not clear what would happen** when the trial period ends, based on the information that was provided to them (29% encountered this often, 25% sometimes). When questioned about cancelling the subscription at the end of the free trial, 54% of consumers considered it to be easy always or most of the time.

Another issue concerns **free trials requiring payment information up-front**, which 90% of consumers responding to the public consultation had experienced and 50% of respondents to the consumer survey encountered regularly. The sweep identified the need to enter payment information in 39.1% of cases where free trials were available. BEUC's

2023 survey also found that 54% of consumers had to register/create an account when making a purchase, going against their preference.

The sweep in the Fitness Check's supporting study also examined issues concerning the **14-day right of withdrawal** from digital subscriptions. Just 54% of traders provided consumers with information about the right of withdrawal at the pre-contractual stage. Even among those that proactively provided such information, only 41.7% presented the information in a manner that could be categorized as 'clear' or 'very clear'. Concerning information about the technical procedures required for consumers to notify service providers of their intention to exercise their right of withdrawal, 50% of traders indicated this at the pre-contractual stage and 56.5% were sufficiently clear in such disclosures, while 8.7% of disclosures were assessed as confusing.

These figures show that the situation has not improved considerably in comparison with the results of the 2019 CPC sweep on the right of withdrawal, which examined 481 e-commerce websites and found that more than a quarter of the websites did not inform consumers how to withdraw and nearly half of the websites were not clear about the time-limit to return the item within 14 days from the moment the consumer notified the trader of their intention to withdraw.

For contract cancellations after the 14-day right of withdrawal period, the sweep for the Fitness Check showed that pre-contractual information on the procedure for cancellation of subscriptions was provided in 69% of cases, but the clarity of such information was assessed as fairly clear only in just 34.7% of cases, which is the same percentages as for 'not clear' and 'not at all clear' disclosure. The clarity of the technical procedure to follow to cancel the subscription was fairly clear in 38% of cases and 'not clear' or 'not clear at all' in 34% of cases.

The **technical procedure to notify cancellation** varied, but in 40% of cases it occurred through the online interface (e.g. a button on the website), 35% required sending an e-mail to unsubscribe and 5% required cancelling the payment as a means to cancel the subscription. In 20% of cases, the procedure was unclear. Examples of lack of clarity included only having contact details for the administrator on the website, or having to enter the FAQ (frequently asked questions) page, followed by having to navigate to a section with questions about subscriptions, and by additional clicks to find a link to start the cancellation.

In addition to the sweep, the consumer survey showed that consumers face barriers when exercising their right of withdrawal. 44% of consumers found it **difficult to even notify traders of their intent to withdraw** from a purchase, with the issue being more pronounced for the 26-35 age group (half of them voicing concerns). 29% of consumers had experienced a situation where they were not able to withdraw from a digital subscription within 14 days of purchasing it (e.g. there was no way to notify the provider about the withdrawal or the provider did not accept the request to withdraw).

Consumers also face barriers when dealing with traders regarding missing reimbursements - 45% encountered difficulties often, while an additional 29% faced these issues sometimes. Younger consumers aged between 18-25 and 26-35 experienced these issues more often, with 52% of those in the 26-35 age bracket and 42% in the 18-25 category reporting difficulties.

Furthermore, 30% experienced a situation where, after successfully withdrawing from a digital subscription, the **trader charged them more than just the amount due for the**

time they used the subscription (e.g. they had to pay for an entire month even though they only used the subscription for a few days before withdrawing).

Overall, this underscores the need for clearer communication and responsiveness from traders to ensure full compliance with the right of withdrawal, which is fully regulated in the CRD. However, it also points at possible legal uncertainty on the side of the traders about their obligations, for instance concerning the compensation owed to them by the consumers on a pro-rata basis in case of withdrawal from the digital subscription contracts.

Legal framework

EU consumer law fully applies to digital contracts and subscriptions that consumers conclude online.

Concerning contract cancellations, in 2023, the revision and repeal of the DMFSD introduced in Article 11a CRD a requirement for traders to provide a prominent and easily legible **withdrawal function** (e.g. button) for all distance contracts concluded by the means of an online interface. Traders must also send acknowledgement of receipt of the withdrawal on a durable medium following the activation of that function. Whereas the CRD provides for the 14-day right of withdrawal from online contracts, EU consumer law does not require any specific cancellation option for digitally concluded consumer contracts beyond the right of withdrawal. In the UCPD Guidance, the Commission considered that it should be as easy to unsubscribe/cancel as it is to subscribe, deriving this principle from the interpretation of Article 9(d) UCPD, which considers barriers to contract termination as aggressive practices.

In addition, the DMA states that a gatekeeper should not apply disproportionate general conditions for terminating the provision of a core platform service, and shall not require end users to subscribe to or register with a core platform service as a condition to use another core platform service of the gatekeeper. The DMA additionally prohibits gatekeepers from requiring end users to use identification or payment services or a web browser engine of the gatekeeper, in the context of any service provided using a core platform service and prohibits gatekeepers from restricting end users' ability to switch between, and subscribe to, different software applications and services that are accessed using the core platform services of the gatekeeper. As highlighted earlier, the DSA's prohibition of dark patterns also covered obstacles to cancellations, but the scope of the provision excludes practices falling under the scope of the UCPD. Furthermore, the DMFSD's prohibition of dark patterns (added in CRD Article 16e) left the Member States with a choice whether to adopt specific measures against obstacles to cancellations and its scope is limited to financial services contracts.

Beyond contract cancellation, the lack of transparency about key aspects of the contract, such as the price or paid nature of the subscription, its duration or renewal, could breach the existing information obligations in the CRD, UCTD and UCPD. Art. 8(2) CRD specifically requires the trader to remind the consumer about the 'obligation to pay' immediately before concluding the online contract and the Payment Services Directive requires explicit information about the payable charges and the consumer's consent before payment.[261]

Furthermore, a contract term that ties a customer into a subscription without making clear the nature of the contract and related conditions, or a term that foresees auto-renewal

[261] This Directive is currently under revision, following the Commission's proposal in June 2023.

multiple times the original price, could be deemed non-transparent and unfair under the UCTD, subject to a case-by-case assessment.

Apart from the above-mentioned provisions, the current horizontal EU consumer law does not expressly regulate automatic renewals, reminders, price hikes, switching from free trials to a paid subscription, requiring payment details for free trials or other aspects. Several practices that were described earlier could be considered problematic by consumers and certain stakeholders. There are some examples of requirements in sector-specific legislation, such as the European Electronic Communications Code, which in Art. 105(3) requires notifications in a 'timely manner' about automatic renewals in case of electronic communications services and regulates other aspects regarding the contract duration and termination.

In the absence of EU rules on contract termination, national contract laws apply. Several Member States have adopted national legislation regulating specific aspects of digital contracts. From 2022 and 2023 respectively, DE and FR require a clear and easily accessible cancellation functionality/button, with two or three clicks, respectively. Different approaches to ensuring consent for automatic renewals were introduced in AT, BE, BG, DK, FR, DE and IT, which also stipulate rules on the timing and form of renewal information provided to consumers. Some Member States only apply the rules to specific types of contracts such as energy provision, insurance, or communications services. DE allows for automatic renewal only if the contract is extended for an indefinite period, i.e. without a further minimum term, and consumers must be given the right to terminate the contract at any time with one month's notice. In addition, clauses stipulating notice periods of more than one month before the end of the initial contract term will be invalid. In FR and IT, any tacit renewal clause must be signed or clicked twice, otherwise the consumer can cancel the contract at any time. BE has specified that the renewal clause must be prominently displayed in a separate box on the first page of the contract, and must clearly state the consequences of the tacit renewal, the final date for opposing it, and the methods for notification of opposition.

Examples of regulatory approaches outside of the EU include the US Restore Online Shoppers Confidence Act (ROSCA) that requires express consent for charges, Californian Assembly Bill 390 that requires easy cancellations and a 2023 FTC proposal on tackling 'negative option' practices like automatic renewals, as well as the 2023 UK's Digital Markets, Competition and Consumers Bill, which introduced detailed rules on subscriptions, including pre-contractual information, reminders of auto-renewals and easy cancellations.

There are several examples of case law and enforcement activities regarding aspects that are regulated at EU level. For example, the Court recently clarified in case C-565/22 that the consumer's 14-day right to withdraw in the CRD is guaranteed only once in case of a contract preceeded by a free trial. In 2021, following a complaint by BEUC, the Norwegian Consumer Council and the Transatlantic Consumer Dialogue, a coordinated CPC action was launched against Amazon Prime concerning the difficulties consumers face with unsubscribing from the digital service. The practices entailed a large number of hurdles, including complicated navigation menus, skewed wording, confusing choices, and repeated nudging. Amazon committed to bringing its cancellation practices in line with EU consumer law, in particular the UCPD. As a result of the action, from 1 July 2022 EU and EEA consumers could unsubscribe from Amazon Prime with two clicks, using a prominent and clear cancellation button (covering desktop and mobile environments). A similar action was launched by the Federal Trade Commission in the US in 2023.

Furthermore, in 2023, under the lead of the Danish Consumer Ombudsman, the CPC network obtained commitments from Mastercard, VISA and American Express to introduce a series of changes to ensure that traders provide clear information to consumers on recurrent payments before they enter into a subscription. MasterCard and VISA also required traders to display the applicable subscription fees in the checkout window where consumers enter their credit card information for their first purchase or first trial leading to a subscription. Intermediaries such as app stores and payment service providers play an important role in ensuring transparency about subscriptions and facilitating traders' compliance with their obligations under consumer law.

Moreover, at national level, there are several examples of case law developments concerning renewals. For example, in 2019, a German court found a 30x price increase following automatic renewal, in addition to placing the consumer under time pressure and baiting them with a test offer, to be unfair.

Stakeholder views

Concerning possible solutions to the identified problems, stakeholders responding to the public consultation supported mandating a **clear technical means for cancellation** (e.g. cancellation button, beyond the 14-day right of withdrawal) (62%) and a **contract termination confirmation** (69%). Many stakeholders considered that if it was possible to conclude the contract via digital means, then it should also be possible to cancel that contract through similar means, without for example speaking to customer service, which could discourage certain consumers. Consumer organisations strongly consider that it is still too difficult to cancel contracts, pointing at dark patterns in interface design and unreasonable cancellation fees. Several traders and business organisations expressed concerns about prescriptive cancellation functions, such as buttons, which may pose technical problems (e.g. implementation in case of virtual assistants) and limit the traders' freedom in terms of interface design. Furthermore, some traders suggest that such solutions may be more feasible for digital content and services, but not for returns of physical products.

Concerning renewals, the EP's 2023 report on video games called on the Commission to introduce an obligation to require consumer opt-in to auto-renewals (instead of having it as a default), coupled with clear and easily accessible information on how to cancel auto-renewals at any time, and requiring the process of cancelling the auto-renewals to be as easy as the sign-up. In the public consultation, there was also majority support for requiring **reminders before automatic renewals** (63%) and **reminders about inactive subscriptions** (59%). Several traders provide such reminders on a voluntary basis; however, some have concerns that while reminders about annual or, possibly, also quarterly subscriptions would be acceptable, consumers might not appreciate receiving monthly reminders or any reminders at all.

There was also support in the public consultation for requiring **express consent when switching from a free trial** to a paid service (67%). In their responses, stakeholders also suggested amendments to make it compulsory to **provide information on the total cost of the subscription** and to highlight the nature of a continuing obligation. Respondents were also in favour of prohibiting mandatory **payment details for free trials** (60%). Looking at the figures per respondent type, 92% of consumers agreed with this, compared with traders or business organisations, where only 12% agreed, whereas 25.9% strongly disagreed. Several traders, in particular representatives of entertainment streaming services, explained that there are valid reasons for requesting payment information or

account creation, such as avoiding the abuse of free trials, including by malicious actors or bots to access, and spread content for free. It was also noted that regulatory changes in this area could have the unintended consequence that traders become more reluctant to offer free trials.

Taking the above into account, EU consumer law cannot be considered effective in addressing the concerns regarding digital contracts and subscriptions, including specifically their cancellation and renewal. Several aspects that raise problems for consumers are not regulated by the Directives and remain subject to national contract laws. Given the wide variety of national approaches, there is currently regulatory fragmentation and a risk of further divergence in the future.

VI.1.6. Unfair contract terms

Problems with unfair contract terms

Consumers have limited bargaining power when entering contracts in the digital environment – in general, they can either take it or leave it. In the public consultation, 62% of consumers indicated having **perceived a contract term to be unfair** when buying a digital service or digital content, but nevertheless had to agree to it. This presupposes that consumers were able to familiarise themselves with the contract terms in the first place, in order to be in a position to assess their content.

The Fitness Check's supporting study confirmed that users of digital services or purchasers of products online **rarely read the Terms & Conditions**. While the issue arises both in online and offline transactions, as already highlighted by the 2016 European Commission study on consumers' attitudes towards T&Cs and 2017 Fitness Check, the specificities of the online environment make it more prevalent online. The EP's 2021 study on terms in contracts of digital service providers shows that this is due to reasons related to the **dematerialisation** of the contract, the **spread of contract terms** across several webpages, in the form of T&Cs, Terms of Service and Policies, Payments Terms of Service and the Privacy Policy, leading to difficulties with locating them online, as well as their reported **length, complexity and/or ambiguity** (e.g. situation where the 'privacy policy' also determines contractual rights and obligations).

Respondents to the public consultation also said that the design of a website or app was confusing, which made them uncertain about their rights and obligations under the contract, with 49% having experienced this problem 3 times or more over a year.

In the consumer survey, only 36% of consumers indicated that they read the T&Cs always or often, with a further 23% indicating they do this sometimes. The likelihood of reading T&Cs increases with the **consumers' age** – only 26% of consumers aged 18-25 indicated they read them regularly or always; this rose to 31% for those 25-36; 34% for those aged 46-55; 40% for those aged 55-64 and 46% for those aged 65+. Consumers who were very **untrusting of online businesses** were less likely to read T&Cs, compared to those who indicated they were **very trusting** (33% vs 48% respectively).

41% of consumers considered that the **presentation and language** of the T&Cs made it difficult to understand the rules that apply and 40% would have liked to read a **summary** of the T&Cs but it did not exist. Moreover, 49% of consumers indicated that it was possible to **agree to the T&Cs automatically** by completing the payment process, by signing up etc., without being prompted to read the terms.

When specifically asked in the consumer survey about the terms or situations they encountered in their online contracts, consumers were able to recall seeing the following, which could be perceived as problematic, subject to a case-by-case assessment by a competent court or authority:

- The contract allowed the trader to keep and process their personal data even after the end of the contract (36%).
- Mere access to the site implied consent to the T&Cs, even if the consumer was not able to have access to the T&Cs at that point (36%).
- The information on the duration of the contract and what happens when it expires was not clear (35%).
- The contract gave the trader the right to collect additional personal data throughout the performance of the contract without the consumer being informed about which data will be collected or given the right to terminate the contract (34%).
- The contract gave the trader unrestricted access to the consumer's personal data which was generated by using their product or service (e.g. to use it for direct marketing or advertising, for determining their credit score, for determining the eligibility for health insurance or for calculating/modifying insurance premiums) (34%).
- The contract stated that the trader was not liable for any disturbance in the availability or reliability of the service regardless of the reason (33%).
- When the contract was automatically renewed, the new contract specified a price that was higher than the price in the original contract without the consumer's consent (31%).
- The contract gave the trader the right to unilaterally delete the consumer's account (28%).
- The contract required the consumer to give up ownership of the content that they create/share on their service (23%).
- The contract terms obliged the consumer to conclude an additional contract concerning digital content or hardware with a third party (23%).

Additionally, the supporting study to the Fitness Check used CLAUDETTE, an experimental Natural Language Processing tool developed by researchers at the European University Institute evaluating terms of service and privacy policies of online platforms and apps, particularly from the point of view of the UCTD and the GDPR. It aimed to detect potentially unfair terms in the T&Cs of 35 websites commonly used by EU consumers (15 e-commerce sites, covering sectors like telecoms, energy, and travel, 15 online platforms, 5 micro-contract operators such as influencers/content creators), followed by manual review to verify the results. The study identified the following **types of contract terms** which are common in the T&Cs examined and raise concerns about user rights and the balance of power between traders and consumers in the digital environment:

- **unilateral termination**: the analysis revealed a significant occurrence across 23 websites of terms granting the trader the right to unilaterally terminate user accounts or access.
- **unilateral change**: the terms giving the trader the right to unilaterally change the contract were found across 30 websites.
- **content removal**: 13 examples of terms related to content removal were identified, providing for the trader's right to edit or remove user-generated content.

- **jurisdiction**: in 13 instances, terms regarding jurisdiction were used and which are either unclear or conferred exclusive jurisdiction to the courts of trader's establishment.
- **limitation of liability**: 8 examples of clauses limiting traders' liability for user experience and outcomes.
- **choice of law**: in 7 instances platforms provided for the choice of law governing the contract, including the law of a non-EU country.
- **arbitration**: 10 terms related to arbitration clauses, specifying the method of alternative dispute resolution. Such terms may be unfair if they force consumers into binding arbitration or deprive them of the right to seek legal recourse in case of disputes.

Additionally, T&Cs of platforms often involve dynamic and rapidly changing terms that can be updated regularly without direct communication with consumers.

These empirical findings confirm the results of prior academic research, for example in 2015, 2019 and 2022 which identified a number of problematic contract terms. For example, **limitation of liability** clauses were present in 98 out of 100 Terms of Service, across all market sectors. The most common practices were general and non-specific limitation and/or exclusion of liability (20%), followed by liability limitation for third-party actions (12%), for any damage (9%), and for interruption and/or the unavailability of the service (8%).

The most common **contract modification** terms, giving the possibility to unilaterally change the contract without giving reasons (60% of all unilateral change contract terms), were found in all contracts in five out of nine sectors (e-commerce, productivity tools and business management, Web search and analytics, health and well-being, and content sharing platforms).

Content removal at the trader's sole discretion was relatively frequent across most sectors, with relevant terms found in over 50% of contracts in seven out of nine sectors, and their presence was especially high for gaming and entertainment and in social networks and dating.

In contrast, problematic **arbitration** terms, relating to the application of extra-legal rules and the place of arbitration outside the consumer's residence, were identified in less than 50% of contracts, which according to the authors could be thanks to the application of the UCTD as interpreted by the CJEU. Finally, the research found that certain terms contained in privacy policies serve to authorize a pervasive collection and AI processing of **personal data**.

The Norwegian Consumer Authority, Forbrukerrådet, investigated the Terms of Services of national and global **cloud storage** service providers (Jottacloud, Telenor Sky, Dropbox, Google Cloud (disk), Microsoft OneDrive). The short study found, for example, that certain contract terms were unclear about what constitutes "normal" or "acceptable" use of their cloud storage service, allowed the service provider to shut down accounts, for any reason, without a warning, or restricted the use of the service beyond the limits of the law.

Similarly, the EP's 2021 study on terms in contracts of digital service providers identified a number of main categories of **potential unfair terms in the digital environment**, covering, for example: i) the **conclusion** of a contract (such as related to browse-wrap contracts and tacit consent), ii) the limitation or exclusion of the **liability** of digital service

providers (such as regarding the modification/ interruption of the digital service, content moderation, unilateral modification of contract terms, loss or damage to the data supplied by the consumer), iii) the **suspension or termination** of the contract (such as regarding the unilateral termination where the consumer's behaviour does not objectively justifies it, the prohibition for consumers to recover the data stored, shared or created by them), iv) the collection and use of the consumer's **personal data** (such as regarding the data minimisation principle under the GDPR or denying consumers the right to withdraw their consent or hindering the use of such a right, e.g. by introducing a complex consent withdrawal procedure or introducing a penalty fee for the withdrawal), v) **dispute resolution** (such as related to mandatory arbitration and jurisdiction clauses hindering consumers from taking legal action or exercising a legal remedy, applicable law clauses depriving consumers of the protection offered by the mandatory law of their country of residence or misleading them about that protection), vi) terms on **copyright** (such as requiring the consumer to grant the digital service provider a license to use the content the consumer has generated on their platform or by using their service).

Finally, BEUC has consistently highlighted the use of similar potentially unfair terms in the digital environment, e.g. in 2014, 2018, 2021, 2022 and 2023.

These findings are corroborated by a 2023 recommendation of the French *Commission des Clauses Abusives*. After examining 64 consumer contracts concluded with online marketplaces and with their third-party sellers, it found 69 unfair terms containing incomplete or misleading information, including terms about the applicable law, jurisdiction or arbitration, and terms limiting the liability of the trader. The *Commission des Clauses Abusives* recommended that such terms be removed from all consumer contracts.

The lack of transparency and fairness in T&Cs can result in **consumer detriment**. In the consumer survey, 21% indicated they had **suffered financial harm** because they did not know all the conditions that applied to their contract. This was particularly high for those consumers who indicated they are highly likely to act on impulse – with figures ranging from 31% of those who act on impulse on a daily basis, compared to only 4% who never act on impulse. It was also particularly high for those who indicated that spending time online has a highly negative impact on their daily life. Consumers also reported other types of losses, such as **lost time** because it was not clear where to find the T&Cs on the website/app (35%), having their **privacy harmed** because they unintentionally agreed to share more personal data than intended (29%), **losing access to the service or to their account** because they did not know the conditions for limiting or excluding their access (23%) or having **difficulties with exercising their rights** because it was hard to understand which T&Cs apply to their contract (32%).

Legal framework

The problems related to consumer contracts in the digital environment highlighted above are covered at EU level by the UCTD. The UCTD, as interpreted by the rich case-law of the CJEU, regulates the **fairness and transparency** of non-individually negotiated terms in consumer contracts, in particular pre-formulated standard T&Cs. Article 3(1) provides for a **general test** to assess the **unfairness** of contract terms, i.e. whether they, contrary to the requirement of good faith, create a significant imbalance in the parties' rights and obligations to the detriment of the consumer. This general test is to be applied by national authorities on a case-by-case basis. In addition, Article 3(3) refers to the Annex to the

UCTD which contains an **indicative and non-exhaustive list** of contract terms that may be regarded as unfair.

The UCTD also contains **transparency** requirements under which contract terms must be drafted in plain, intelligible language (Articles 4(2) and 5) and consumers must be given a real opportunity to become acquainted with contract terms before the conclusion of the contract (point 1(i) of the Annex). Contract terms whose meaning is unclear must be interpreted in favour of the consumer, and contract terms which are not transparent and do not allow consumers to understand their rights and obligations under the contract may be considered as unfair. Finally, the CJEU clarified, e.g. in Joined Cases C-776/19 to C-782/19 *BNP Paribas Personal Finance SA*, that transparency also entails a **positive information duty for the trader** and the **burden of proving** that a contract term is transparent cannot be borne by the consumer.

Under Article 6 (1), unfair contract terms are **non-binding on the consumer**, the CJEU ruling that this constitutes a mandatory rule of equal standing to the rules of public policy laid down in the law of the Member States, for example in Case C-488/11 *Asbeek Brusse*. Consequently, the determination by a court that a contract term is unfair must, in principle, have the consequence of **restoring the consumer** to the legal and factual situation that he or she would have been in if that term had not existed, including the restitution by the trader of the amounts paid by a consumer based on unfair terms, as held iteratively by the CJEU, for example in Case C-520/21 *Bank M.*.

The UCTD is a principle-based, **minimum harmonisation** instrument. As such, it sets a minimum EU level of consumer protection and allows Member States to provide more protective consumer protection rules in their national legislation, i.e. a broader scope of the national rules transposing the UCTD, or more detailed or stricter rules regarding the unfairness of contract terms. The study supporting the 2017 Fitness Check and the information (website last updated on 31 May 2019) showed that several Member States have used this possibility by, for example, introducing '**blacklists**' of unfair terms (contract terms considered unfair in all circumstances) and/or '**grey lists**' of contract terms (terms presumed to be unfair unless proven to the contrary). For example, NL law contains a blacklist, a form of a grey list (i.e. a list of contract terms which may be considered as unfair), as well as a 'blue' list ("an indication that the contract term should be paid attention to"). BE, BG, CZ, DE, EE, EL, ES, FR, IT, LU, HU, AT, PL, PT and SK also have implemented some forms of blacklists or grey lists. Some MS, such as BE and CZ, have applied the national law transposing the UCTD also to individually negotiated contract terms. Other MS, e.g. PT, FI and SE, have extended the application of national law transposing the UCTD to terms on the adequacy of the price and the main subject even if those terms are transparent.

These rules apply to the potentially unfair contract terms identified by this Fitness Check. Some of these terms are present both offline and online and the UCTD has already been interpreted in their respect by the CJEU. In addition, the experience of national enforcers and courts, as well as of the CPC network, show that the UCTD can also successfully capture new, potentially unfair, contract terms that are specific to digital environments, such as related to the unilateral removal or editing of user-generated content, the 'freemium model' where consumers are misled about their need to share personal data or dedicate time and attention to advertisements, the limitation of liability of digital service providers and the excessive collection of consumer data.

For example, terms related to **jurisdiction and arbitration** are likely to fall within the category of terms which have the object or effect of excluding or hindering the consumer's right to take legal action, referred to in paragraph 1(q) of the Annex to the UCTD. In Case C-519/19 *Ryanair DAC v DelayFix*, the CJEU held that a non-individually negotiated term in a consumer contract concluded online, which confers exclusive jurisdiction on the courts which have jurisdiction over the territory in which the trader is based, must be considered as being unfair within the meaning of Article 3(1) UCTD.

As regards terms related to the **choice of law**, in Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl*, the CJEU held that a non-individually negotiated term, under which the contract concluded with a consumer in the course of electronic commerce is to be governed by the law of the Member State in which the trader is established, is unfair under Article 3(1) UCTD in so far as it leads the consumer into error by giving them the impression that only the law of that Member State applies to the contract. The CJEU confirmed in Case C-455/21 *Lyoness Europe AG* that, under Article 6 (2) UCTD, contract terms cannot deprive consumers of the protection afforded by the UCTD by virtue of the choice of the law of a non-EU country, provided that the contract has a 'close connection with the territory of the Member States'.

Concerning contract terms related to the **limitation of liability**, for example, in 2021, the Italian consumer protection authority concluded separate proceedings against Google Drive, Dropbox, and iCloud Apple. The decision considered unfair, based on the UCTD as transposed in Italian law, the contract terms excluding any liability for the malfunctioning or failure of a service, as well as for damage caused to the device and the uploaded data, placing the entire risk on the consumer, and excluding any protection or right of the latter. These terms exempt the supplier from liability for any error or malfunctioning that may occur, with the consequence that the consumer cannot claim any compensation in the event that they suffer any damage during use of the service (e.g. loss of data, interruption of activities, etc.), unless there is wilful misconduct or gross negligence on the part of the digital service provider in breach of the terms of service. The decision further considered unfair the possibility for the traders to **modify unilaterally** the T&Cs and to **suspend/interrupt** the service.

More generally, under the revised Product Liability Directive, manufacturers, including software companies can be held liable in case of destruction or corruption of someone's data by their defective product. Any contractual terms that would exclude or limit the liability under the directive are forbidden (Article 15).The *Tribunal de Grande Instance* of Paris, France, ruled in 2018 and 2019 in various actions for injunctions challenging hundreds of T&Cs used by Twitter (judgment of 7 August 2018, n° 14/07300, largely upheld by the Court of Appeal of Paris, judgment of 14 April 2023, n° 19/09244), Facebook (judgment of 9 April 2019, n° 14/07298) and Google (judgment of 12 February 2019, n° 14/07224), brought by the French consumer protection organisation UFC Que Choisir. The French court analysed these terms in light of consumer legislation, and in particular the national rules transposing the UCTD, and data protection rules, and found that a high number of terms were unfair and invalid. The court ruled in particular that the **collection of personal data** was not sufficiently transparent, omitting informing users that the collection of personal data had a commercial value and would be used for such purposes. This prompted the conclusion that users' explicit consent should be incorporated into the contract itself, rather than relegating it to the T&Cs for using the service.

Furthermore, the court emphasised the necessity for users to provide a new agreement in the event of substantial amendments to privacy policies and terms of use. This underscored

the importance of keeping users informed and obtaining their **explicit consent for any significant changes** to the contractual framework. Moreover, the trader could not **suspend/delete an account** without justification or recourse and could not exclude any **liability** on the part of the online service provider. The provider could not reserve the right to **change their conditions**, or to **terminate the provision** of the service, without indication on which grounds such measures could be taken.

Conversely, the court considered that the presentation of the Terms of Use and the Privacy Policy in two documents provided consumers sufficient information to grasp the nature and scope of their obligations and rights, while the use of hyperlinks and 'fragmentation' of relevant information was suitable to avoid an excessive concentration of information in a single text in limited space, the wording was sufficiently informal and included a glossary, and the personal nature of the information processed was sufficiently highlighted.

In 2020, the *Tribunal Judiciaire* of Paris, France, found that a number of terms used by Apple in the T&Cs of iTunes, then Apple Music, were unfair (judgment of 9 June 2020, n° RG 16/09799). In particular, it addressed the terms using imprecise expressions or non-exhaustive lists of the purposes for which **personal data** would be collected and processed, since they gave in essence to the trader the unilateral right to interpret these terms.

The CPC network carried out a number of investigation and enforcement actions to tackle widespread breaches to UCTD in the digital area, in particular as regards social media and search engines as well as market places and digital services. The CPC sent a common position to Facebook, Twitter and Google+ in November 2016 asking them to improve a number of contract terms. Since then, social media operators specifically agreed to amend the terms of services limiting or totally excluding the liability of social media networks in connection with the performance of the service; the terms requiring consumers to waive mandatory EU consumer rights, such as their right to withdraw from an on-line purchase; the terms depriving consumers of their right to go to court in their Member State of residence, and providing the application of California law; and the term releasing the platform from the duty to identify commercial communications and sponsored content. The enforcement action led to further changes to their T&Cs in 2018, and in 2019 Facebook had to implement additional amendments to its T&Cs as regards its policy on limitation of liability, which now acknowledges its responsibility in case of negligence, for instance in case data has been mishandled by third parties; its power to unilaterally change T&Cs by limiting it to cases where the changes are reasonable also taking into account the interest of the consumer; the rules concerning the temporary retention of content which has been deleted by consumers; and the language clarifying the right to appeal of users when the their content has been removed.

A 2023 CPC common position addressed the unfair and non-transparent terms used by Google to retain the power to unilaterally cancel orders and change price mistakes in its "Google Store Terms of Sale for Devices".

Similarly, PayPal has committed to modifying its T&Cs to make them more transparent and easier to understand for consumers as from 28 May 2024, including as regards: terms requiring consumers to check the compliance with the law (for example, wording such as 'to the extent permitted by law'); terms implying that consumers are liable for damage not caused by their fault or that could not have been foreseen; terms obliging consumers to verify the information themselves (such as stating that PayPal cannot guarantee the accuracy of the information); and terms related to jurisdiction and the applicable law.

Finally, in 2021 and 2022, further to a CPC coordinated action, the Chinese marketplace AliExpress committed to clarify their T&Cs for consumers as regards jurisdiction, the possible application of additional costs linked to customs clearance, the applicable rules and consumer rights such as the right to cancel, and the right to a refund. AliExpress further committed to inform consumers in advance about any changes to the T&Cs and give them the opportunity to cancel the contract on the platform.

The existing case law and enforcement actions show that the UCTD can be used successfully to tackle the most prevalent issues related to transparency and fairness of contract terms in the digital environment. However, they also show that enforcement actions have not rooted out all non-transparent and unfair terms in the digital markets even in the case of the actors that were subject to such actions, the causes being multiple.

First, while the principle-based nature of the UCTD makes it **applicable to any possible term** in a consumer contract in the digital environment, and thus **future-proof**, the downside is that there are cases in which it is perceived to provide **insufficient clarity about its applicability**. In particular, stakeholders pointed to the fact that the UCTD Annex items are worded in **general** terms, without specific indications about how they apply in digital contexts. Some stakeholders also indicated that the possible application of the UCTD to **personalised terms**, customised unilaterally by the trader, is not fully clear either, since certain market actors tend to consider such terms as being individually negotiated and thus not covered by the UCTD.

In addition, an academic considered that using the current **'average consumer'** benchmark in respect of the **transparency** assessment under Article 5 UCTD sets the bar too high in light of the actual behaviour of consumers online and entails the risk of lowering the consumer protection under the UCTD. This opinion seems supported by the research mentioned above with regard to the difficulties faced by consumers to read and understand the T&Cs in the online environment. Moreover, the **restitutory effect** based on economic harm incurred and restoring the consumer's factual position in the absence of the unfair term are more difficult to operationalise by national courts in the case of digital trade, for example in the absence of a pecuniary exchange in the case of registration to social networks.

The study supporting the Fitness Check found that these issues **hinder enforcement** by national authorities and courts or **dissuade consumers** from taking any action. For example, a national consumer association reported that some consumers may not seek redress about problematic contract terms because they do not understand their rights clearly when digital services seem to be provided for free, since it is not clear to them that they have entered a consumer contract. Similarly, an academic argues that some consumers may mistakenly believe that some terms are enforceable, when they are in fact unfair, and as such, would not seek legal redress. The public consultation confirmed that, while over half of the respondents had experienced a problem with an unfair contract term, though it was not necessarily indicated as the most serious problem faced in the digital environment, 79% of the respondents said that they did not take any action, such as lodging a complaint or legal action.

In addition, several stakeholders recognised that enforcement efforts at EU and national level focused less on contract terms than on commercial practices. One national consumer authority reported that this was the result of a **prioritisation strategy** reflecting comparative enforcement effectiveness, and that comparatively fewer resources were placed on the monitoring of unfair contract terms. However, given the new challenges that

are specific to the digital environment, the study supporting this Fitness Check found that national ministries are generally satisfied with enforcement under the UCTD and the national transposition laws, even if several ministries and enforcement authorities referred to challenges regarding the length of negotiation and/ or redress procedures for online actors to come into compliance.

In the case of cross-border infringements, stakeholders also considered that the **fragmented** nature of the enforcement system was a limitation given the cross-border dimension of B2C transactions in the digital environment. An additional challenge arises in **collective actions**, such as based on the Representative Actions Directive, where various national laws transposing the UCTD may be applicable depending on the consumers concerned by the action. This is in particular because the new problems affecting the fairness of contract terms in the digital environment are not addressed specifically and explicitly by the UCTD and national standards may differ. In an online environment where market borders do not exist, certain stakeholders perceive this as problematic.

Stakeholders, including several ministries and enforcement authorities, also highlighted the **limited deterrent effect** of the UCTD, especially for global digital players, in the absence of substantial **sanctions** despite the new provision on penalties. For example, in 2019 the Paris Tribunal de Grande Instance ordered Facebook to pay UFC Que Choisir the sum of EUR 30 000 as compensation for non-material damage to the collective interests of consumers by the use of more than 400 unfair or unlawful terms in its T&Cs. Similarly, in 2023 the Paris Court of Appeal ordered Twitter to pay UFC Que Choisir the sum of EUR 50 000 as compensation for the use of over 200 unfair or unlawful terms in its T&Cs. One stakeholder reported that the amount was insignificant, and thus not deterrent, compared to Facebook's revenues and the magnitude of the infringement, while the investment made by the French consumer association was substantial, given major imbalance in resources available to both parties.

The deterrent effect of sanctions has been addressed to some extent by the Modernisation Directive which required Member States to provide for turnover-based penalties for the breaches of the UCPD, UCTD and CRD. However, these stronger penalties are mandatory only for cross-border infringements that are subject to the CPC coordinated action, which some stakeholders consider to be very demanding. Some stakeholders were also concerned about the application of penalties to infringing actors established in **third countries**. Further improvements regarding the enforcement in cross-border cases and penalties, including vis-à-vis non-EU traders, could be made in the framework of the possible reform of the CPC Regulation.

More generally, stakeholders also pointed to the lengthy procedures (several years) and significant investments required when seeking redress, through court action, to bring traders into compliance. In their view, this undermines the practical enforceability of the UCTD, also given the limited deterrent effect of the sanction regime, despite improvements introduced by the Modernisation Directive.

Concerning coherence with new legislative developments in the digital area, the UCTD applies to all consumer contracts in all sectors of economic activity, in addition to other relevant provisions of EU law that may also apply in parallel depending on the type of contract in question, as ruled by the CJEU e.g. in Case C-92/11 *RWE Vertrieb AG*. The CJEU clarified, e.g. in Case C-290/16 *Air Berlin*, that the UCTD would not apply in an area governed by another EU instrument only if such exclusion is clearly provided for by the provisions of that instrument.

The DSA introduced additional consumer protection in B2C contract terms, that is applicable in parallel to the UCTD (Recital 10 and Article 2(4)(f)). In particular, Article 14 DSA provides that intermediaries should include information on any restrictions regarding the use of their service in the T&Cs (e.g. policies and tools for content moderation). This information should be in "clear, plain, intelligible, user-friendly and unambiguous language" and publicly available in an easily accessible and machine-readable format. They also have to inform users of significant changes to the T&Cs. When the intermediary service is mainly directed at minors, T&Cs should be explained in a way that is understandable for minors. VLOPs and VLSEs have to provide a T&C summary and publish the T&C in all official languages of the Member States where they provide services. The DSA introduces a set of more specific requirements regarding T&Cs for intermediaries, VLOPs and VLSEs, including on certain aspects related to their transparency and better comprehension by consumers.

The DSA provision on T&Cs and the UCTD are complementary and do not contradict each other, even if some differences can be observed. The UCTD applies to all traders, regardless of their size, whereas certain requirements under the DSA apply only to intermediaries of a certain size. The UCTD's scope is limited to standard non-individually negotiated terms, whereas the DSA applies both to individually and non-individually negotiated terms. The UCTD, as interpreted by the CJEU, could lead in certain cases to the remedy of non-bindingness of unfair contract terms that were not sufficiently transparent, whereas in the case of the DSA the non-compliance with these provisions could be subject to enforcement actions by national authorities or by the Commission, with the possibility of imposing fines up to 6% of the global turnover of the provider. Moreover, the UCTD covers all aspects of transparency of contract terms and is not limited to the aspects covered by Article 14 DSA.

Under Article 17 DSA, providers of hosting services, including online platforms, have a duty to give clear and specific reasons to consumers when they impose any restrictions on the recipients of the service, such as the suspension or termination of the provision of the service or of the consumer's account, on the grounds that the information provided by the recipients of the services is illegal or incompatible with the T&Cs. The relevant information must be clear and easily comprehensible and as precise and specific as reasonably possible under the given circumstances and allow consumers to effectively exercise the possibilities for redress under Article 17 DSA.

Under Article 23 DSA, as regards the protection against misuse of the service by consumers, providers of online platforms are required to set out, in a clear and detailed manner, in their T&Cs their policy and give examples of the facts and circumstances that they consider when assessing whether certain behaviour constitutes misuse and the duration of the suspension.

These provisions are also complementary to the UCTD, while strengthening and making more concrete, within their scope of application, the requirement stemming also from the UCTD that traders cannot use contract terms that give them the right to dissolve the contract or to decide unilaterally to alter the characteristics of the service to be provided on a discretionary basis.

In 2023, in the context of the P2B implementation the Commission published a database of T&Cs from key intermediary service providers, including terms applicable in B2C contracts. The database includes a variety of documents such as Commercial Terms, Developer Terms, Live Policy, Terms of Service, Privacy Policy etc. The availability of

these terms could help monitor changes in T&Cs and facilitate enforcement, thereby increasing also the effectiveness of the UCTD in the digital area.

The DMA also explicitly applies without prejudice to the UCTD, as stated out clearly in Recital 12. It does not directly cover the fairness of terms in consumer contracts but does include provisions that prohibit gatekeepers from imposing the use of their services on consumers, as well as from making the termination of use of a service disproportionately difficult. Under Article 8 gatekeepers have an obligation to ensure that the measures they implement based on the DMA comply with consumer law, including the UCTD. More specifically, under Article 5(6) DMA, gatekeepers are under a clear obligation to not prevent consumers from raising issues with public authorities, including national courts. This prohibition mirrors point 1(q) of the indicative list of unfair terms in UCTD Annex which refers to contract terms excluding or hindering the consumer's right to take legal action or exercise any other legal remedy. Thus, the UCTD and DMA are fully coherent on that account. Article 6 DMA lays down certain obligations and prohibitions including on consumer choice, barriers to contract termination, switching and portability of data, which also apply to gatekeepers' T&Cs. Any infringement or restriction of consumer rights stemming from this provision by way of contract terms could also be challenged under the UCTD.

The Data Act also complements and is without prejudice to the UCTD, as provided in its Article 1(9). It lays down certain information requirements, such as in Articles 3 to 6, 23, 25, 29 and 36 regarding the obligation to make IoT product data and related service data accessible to the user, rights and obligations regarding IoT data access and sharing, as well as switching data processing services (cloud providers) and essential requirements regarding smart contracts for executing data sharing agreements. Compliance with these requirements is an element that needs to be taken into account when assessing the transparency and fairness under the UCTD of any contract term related to those matters.

Finally, the national case law and enforcement actions mentioned above showed how, in practice, the GDPR is already applied in parallel with the UCTD and contract terms that hinder consumer rights under the GDPR (for example, see a 2018 academic report) can be assessed for their transparency and fairness under the UCTD.

While the Fitness Check has not identified substantive incoherences between the UCTD and the new EU legislation adopted in the digital area, one issue in the area of consistency appears to be their enforcement by the different enforcement authorities. This problem was already highlighted by the 2017 Fitness Check as regards the interplay of horizontal consumer legislation with sectoral legislation, and it seems compounded by the new enforcement architecture under the new EU legislation.

Stakeholder views

Concerning possible solutions to the identified problems related to the assessment of the fairness of contract terms in the digital environment, stakeholders pointed to the fact that the UCTD Annex items are worded in general terms, without specific indications about how they apply in digital contexts, and they would welcome that the **Commission guidance** on the UCTD integrate further specificities of the online contractual environment. In that connection, the study supporting the Fitness Check points to support measures at national level, especially for smaller traders, who reportedly can copy-paste T&Cs from existing websites, such as the contract templates developed in IT. Another reported support measure is a certification process in NL, resulting in a trust mark to online

traders in order to guarantee online customers that they have been audited and are compliant with the applicable legislation, including the UCTD. Such national initiatives have also the advantage of integrating the specificities stemming from national law.

Stakeholders have overall seen the **general unfairness test** under the UCTD as highly effective and relevant to the digital environment and consider that it should remain untouched. However, stakeholders also point out that more legal certainty is needed at EU level in particular as regards the fairness assessment, considering that digitalisation allows a trader to potentially reach consumers in all MS.

Thus, many stakeholders such as consumer organisations (e.g. BEUC in 2021, 2022 and 2023), academic research (e.g. the European Law Institute), the EP (2021 study), but also certain national authorities call for the establishment of a **blacklist of unfair terms in the UCTD** that would cover the unfair terms that are prevalent in the digital environment. That would facilitate compliance by online traders with the UCTD, and its enforcement by national authorities, and avoid fragmentation in the single market since, in the digital environment, markets are less likely to be exclusively or mainly national. As explained above, particular attention should be given to categories of terms related to unilateral changes, content removal, jurisdiction, limitation of liability, choice of law, and arbitration, as well as to data collection, processing and sharing.

At the same time, the findings of the study supporting the Fitness Check indicate that MS **support the minimum harmonisation** nature of the UCTD, which allows them to better protect consumers in certain instances, in particular as regards the development of any blacklists or grey lists of contract terms. There are various reasons, such as the fact that some contract terms are used nationally and are specific to a given MS, and the fact that contract law is a national competence. Other stakeholders, such as consumer ombudsmen, industry associations and legal academics, have also pointed to legal impediments to greater harmonisation in contract terms stemming from the fact that contract law is a national competence. One MS even called for not opening the UCTD at all, as the national blacklist has been developed over 30 years, also according to the rich national case law. The MS was satisfied with the fact that MS retain flexibility to establish national blacklists and update them with any new unfair standard contract term, e.g. those identified through national or CJEU case law or flagged by enforcement authorities, which was seen as having strengthened the Directive's effectiveness.

As a possible solution to the considerable difficulties that consumers have reading and comprehending contracts, 63% of stakeholders in the public consultation supported a **summary of the key terms**, which would in their view be helpful in this respect. The behavioural experiments conducted in the consumer market study to support the 2017 Fitness Check found that standard (long) T&Cs were read less thoroughly by participants than summarised T&Cs, that participants read a higher proportion of the text of the summarised T&Cs, and were better able to distinguish between fair and unfair T&Cs, when presented with summarised T&Cs. On the basis of the findings of the 2017 Fitness Check, discussions facilitated by the European Commission led in 2019 to the adoption by a number of business organisations of recommendations on voluntary ways to improve the presentation of mandatory consumer information requirements and to make more readable and accessible to consumers the standard T&Cs in the online context.

However, further mandatory rules regarding the transparency and presentation of standard contract terms are unlikely to solve the problem of information asymmetry between the contracting parties or lead to the majority of consumers reading the T&Cs and would add

administrative burdens for traders. It would be challenging for traders to identify the 'key' terms among all the T&Cs in case of horizontally applicable consumer law, in contrast to sector-specific rules, in particular since both general consumer law and sector-specific rules can apply at the same time to a given consumer contract. Moreover, in addition to the challenges for consumers to read and understand T&Cs highlighted above, consumers typically cannot negotiate T&Cs and do not have other choice than to accept the terms offered by the trader if they wanted to purchase the underlying product or service, while competitors often offer similar terms. This can be considered as reducing the benefits of reading T&Cs, as found by the 2016 study on consumers' attitudes towards T&Cs. Finally, not having read the T&Cs does not necessarily deprive consumers of their rights, since a significant number of B2C contractual issues are regulated by mandatory consumer law and T&Cs must operate within its boundaries. Conversely, a summary of the key terms can pose risks for consumers. An academic submission to the public consultation highlighted the possible concerns associated with traders such as social media platforms turning legal clauses into oversimplified and less formalistic statements, which can lead to the reduction of legal certainty and the possibility of consumer manipulation.

Another solution to the challenges for consumers to read and understand T&C highlighted above, as proposed by certain academics, could be to move away, when assessing their transparency, from the standard of the 'average consumer' understood as a model individual who is reasonably observant, attentive, and circumspect, which is used by the CJEU even if it is not required by Articles 4(2) and 5 UCTD. In that connection, a legal academic responding to the targeted consultation pointed to an inconsistency in the UCTD in comparison with the UCPD regarding the way in which transparency requirements have been integrated into the two Directives and the relative weight given in the transparency test to an **'average consumer'** as opposed to the concept of a **'vulnerable consumer'**. A legal academic interviewed for the Fitness Check supporting study considered that the 'average consumer' benchmark would be insufficient to protect consumers and that digital consumer vulnerability should be considered when assessing the transparency of a contract term under Article 5 UCTD, which would reflect consumers' varied reactions to the use of AI and algorithms to influence their decision-making.

As regards possible solutions to **strengthen the enforcement** of the UCTD and improve the directive's **deterrent effect**, some stakeholders suggested testing the feasibility of putting fines against major global players on a par with those available under the GDPR and competition policy, ranging in millions of euros, blocking websites, and voiding the contract using unfair terms. In light of the limited resources of national authorities and courts, another recommendation was to further engage traders both at national and EU level in 'preventive' or 'positive' enforcement, i.e. negotiations and dialogue to address consumers and enforcement authorities' concerns, or co-operative preventive work with traders, as is the case already in certain MS, e.g. NL. Finally, providing at national level further information to SMEs on their obligations under the UCTD was considered necessary, as well as promoting existing EU support measures, such as Consumer Law Ready, an EU-wide training programme in consumer law for SMEs.

In conclusion, all types of stakeholders consider that the unfairness test and transparency principles introduced by the UCTD remain useful in a digital environment and should remain in place. Stakeholders (e.g. ministries, consumer protection authorities, industry associations, traders) further indicate that the UCTD has provided regulatory stability and certainty for over 30 years. However, additional guidance and certain updates to the UCTD may need to be explored in light of new challenges in the digital environment, in particular

regarding the establishment of a possible blacklist of unfair terms in the UCTD. More generally, all types of measures, including practical support and training at the national and EU levels, should be explored to improve the transparency of contract terms as regards their presentation and intelligibility. Furthermore, strengthened penalties and additional coordinated cross-border enforcement, as well as further engaging traders in negotiations and preventive dialogue to address consumers' and enforcement authorities' concerns could incentivise online service providers to ensure stronger compliance.

VI.1.7. Automated contracting

Market developments on automated contracting

As new technologies such as smart contracts[262] (on the blockchain) and AI are evolving, they increasingly enable the conclusion and performance of contracts without the need for human intervention. These technologies have varying levels of autonomy: from executing logic and rule-based instructions pre-defined by humans (e.g. smart contracts) to highly autonomous AI systems that learn from data and can recommend and take independent decisions (based on machine learning).

While various use-cases are emerging in B2B context, the most prominent use-case in B2C transactions is consumer shopping, facilitated by automated virtual assistants[263] that can provide information, make recommendations and take transactional decisions. Consumers and traders can use software tools to automate aspects of B2C contracting over the contractual life-cycle. These automation tools can be based on different technologies, functionalities and have different degrees of autonomy. They can be made available to consumers as stand-alone digital services or incorporated in smart IoT devices (e.g. a printer software can enable the consumer to re-order automatically new printer ink from the supplier of the printer when it runs low). Automation tools can also **assist the consumer in navigating traders' offers and making purchases**.

In the future, more sophisticated AI-powered systems could act on the basis of information collected by sensors and **place orders with a greater level of autonomy**. Some types of automation tools such as digital assistants providing information or recommendations are already present on the market whereas more sophisticated ones, such as autonomous AI-enabled tools that can take decisions independently, are not yet widely available in B2C markets.

Potential problems relating to automated contracting

Currently, there is some degree of uncertainty as to the kinds of automation tools for consumer contracts that are likely to be rolled out and the extent to which consumers would use them. For these reasons, data about current consumer problems in this area is limited. However, the Fitness Check points to risks for consumers regarding a broader deployment

[262] Art. 2(39) of the Data Act defines 'smart contract' as a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering.
[263] Art. 2(12) of the DMA defines 'virtual assistant' as a software that can process demands, tasks or questions, including those based on audio, visual, written input, gestures or motions, and that, based on those demands, tasks or questions, provides access to other services or controls connected physical devices.

of automation tools with more advanced functionalities including decision-making functions in the near future.

First, the use of the automation tools implies **consumers giving up, to a smaller or larger degree, the control that they otherwise exercise** when concluding their online contracts manually. The automation tools could be designed in a way that restricts consumers as regards the control they want to exercise, for example, whether to approve any specific contract before it is legally concluded via the automation tool, or to exercise control ex-post, such as by retaining the possibility of stopping the transaction before it is finalised by the automation tool during a given period after receiving a notification from the tool. Highly autonomous AI systems can be designed in a way that, once enabled, they can take independent decisions based on machine learning, over which consumers would have no or extremely limited control.

In the consumer survey, **15% of consumers indicated that they had often experienced a situation where they were charged for a purchase they did not intend to make when using a virtual assistant** (e.g. unknowingly entered into a paid subscription). Consumers could also face technical or even contractual hurdles to suspend or disconnect the automation tool in the situation where they change their mind and wish to return to the traditional online contracting. The plea for more control was also raised in BEUC's 2023 survey, which found that 76% of consumers want more control over how much data smart devices collect about them and 77% want to be able to turn off the internet connection of such devices, if it is not necessary for its core functioning.

Furthermore, automation tools **could lack transparency about their key features**, such as about the identities or limited range of suppliers that the tool interacts with, and the criteria used by the tool for selecting the products and suppliers. Moreover, consumers may face the risk of **these criteria not being objective and giving undue preference to suppliers affiliated with the provider** of the automation tool. A risk typical for automated tools with higher level of autonomy is unexpected and unintended outcomes.

Risks could also arise due to integrity breaches of the automation tools. As highlighted in the context of other commercial practices, there are broader concerns about a lack of transparency on how the consumer's personal data is used. For example, the Commission's 2023 study on the provision of information to consumers about the processing of vehicle-generated data showed that only 38% of consumers are aware that these vehicles collect data and even fewer understand how it is used (31%). To improve transparency, BEUC calls for a new obligation in the CRD on sellers to provide, at the point of sale, information related to the use of personal data by a smart device in a standardised and comparable manner. It may also be relevant for the consumer to know, at the point of sale, whether the smart device requires an app, a stable internet connection or a subscription to function as intended and whether a smart product could function in a data-free-collection mode.

Another relevant aspect in this context will be the **practices of the traders (suppliers) that the automation tool will interact with** for concluding contracts on the consumers' behalf. Whilst it can be expected that online traders will normally have a commercial interest to accept and enable automated contracts, some traders may prevent the access of automation tools to their online interfaces. Traders could also have legitimate grounds for restricting the automated contracting as they may want to be reassured that the automation tool has the consumer's mandate to conclude the contract. For example, they could require the consumer's direct intervention to confirm the transaction initiated by the automation

tool. Such safeguard measures can be beneficial also for consumers, as unwanted automated contracts would also harm the consumer. Furthermore, traders addressed by the automation tools could apply discriminatory treatment to consumers using the automation tools or even provide for the invalidity of automated contracts in their general T&Cs. In other cases, the traders' online interfaces may be inaccessible due to a lack of machine-readability or technical interoperability with the automation tool.

Legal framework

In parallel to this Fitness Check, the Commission has undertaken several studies to explore the specific legal **challenges raised by autonomous AI-enabled contracting and smart contracts** in more detail, both in B2B and B2C contexts.[264] The European Parliament's 2020 resolution on adapting commercial and civil law rules for commercial entities online requested the Commission to assess the development and use of distributed ledger technologies and smart contracts, including in terms of providing further clarifications on the CRD's application, e.g. whether smart contracts fall within the exemption of Art. 3(3)(l) CRD and how the right of withdrawal functions.

Furthermore, between 2022-2025 the European Law Institute works on developing guiding principles and model rules on algorithmic contracts, which includes an assessment of the fitness of EU consumer law for automated decision-making (ADM).[265] Their 2023 interim report identified several points of legal uncertainty in the three Directives, which would require mostly minor adjustments to remove any potential legal obstacles. Overall, there were no significant concerns reported about the ADM-readiness of the UCPD, CRD or UCTD. However, this is without prejudice to the possible need for additional consumer rights or clarifications of traders' obligations, including beyond these instruments or issues not regulated in EU law. The ELI interim report flagged different concepts of the UCPD, such as 'material distortion', 'undue influence' and 'transactional decision', which could be further clarified to include scenarios where unfair practices are deployed on or through the digital assistant. Additional duties to disclose essential information could be considered in the CRD and UCPD, e.g. on what criteria are used by the digital assistant when selecting options. Additional rights could include a right to use digital assistants for contracting and a duty to inform about the use of digital assistants. Concerning the UCTD, there may be a need to clarify that the contract terms should be in a machine-readable format in order for the digital assistant to process them and to allow terms negotiated by a digital assistant to be challenged for their fairness. Additional unfair contract terms could be added to the UCTD Annex: a) a term requiring the use of digital assistants by a consumer to conclude a contract; b) a term permitting the use of only a restricted set of available digital assistants as determined by the trader; c) a term prohibiting the use of digital assistants by a consumer or providing for the application of different terms depending on whether a consumer uses or does not use a digital assistant.

The principle-based and technology-neutral rules of the UCPD and UCTD will continue applying also to contracts concluded with the help of the automation tools and to related

[264] The publication of the studies is forthcoming, with an expected publication date in 2024 for the Study on civil law rules applicable to smart contracts. The studies on Novel forms of contracting in the digital economy (with a focus on AI) are also expected in 2024.

[265] In February 2023, the Institute also approved and published ELI Principles on Blockchain Technology, Smart Contracts and Consumer protection. The reflections on principleshttps://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf for automated decision-making in the EU are ongoing since 2022 and the final deliverables in this work strand are expected at the end of 2024.

commercial practices. The provisions of the e-Commerce Directive could be clarified to explicitly cover automated contracting. The service enabling the consumer to conclude contracts through a digital assistant could be qualified as an information society service. The question of attribution of the actions of an automated tool deployed by a consumer could also be clarified, so as to ensure that consumers using digital assistants can benefit from the protection of EU consumer law. Furthermore, clarifications as to under which conditions a contract is validly concluded with the help of the automation tools, especially highly autonomous ones, and attributed to the persons using them may be useful. Finally, the provisions of the e-Commerce Directive on correcting errors/mistakes may benefit from an adaptation to the technical progress in terms of automated, especially autonomous contracting.

Thus, consumers using automation tools will also benefit from all the consumer rights regarding the product acquired, such as the legal guarantee of conformity under the Sale of Goods Directive and the right of withdrawal under the CRD. The essential pre-contractual information for distance contracts under the CRD would remain relevant also for the 'decision-making' done by the automated tool that will require information about aspects such as main characteristics and price of the products. However, challenges are likely to emerge in practice, as highlighted by a German court case regarding the Amazon Dash button,[266] where the Higher Regional Court Munich considered that the device did not inform consumers sufficiently about the ordered goods and the price.

Some of the information and formal requirements under the CRD, such as the information about the right of withdrawal or the legal guarantee, or regarding the presentation of the "buy" button on the online interface, would not be practically relevant for contracts concluded via the automation tool. In this context, the question arises whether traders should still be obligated to comply with all the applicable information and formal requirements in case automated contracts, especially autonomous ones are used.

In any event, whereas some types of the mandatory consumer information may not be relevant at the time of concluding the contract by the automation tool, they will remain relevant for the consumers in the post-contractual phase. That is why the obligation of a contract confirmation for online contracts on a durable medium, which is typically provided by e-mail, would remain highly relevant for consumers, to enable them to keep track of the contracts concluded and to facilitate the exercise of their post-contractual rights.

Furthermore, specific automated technologies – notably smart contracts (based on distributed ledger technology (DLT)) could pose additional challenges of compliance with certain requirements of EU consumer law due to their technical specificities. For instance, smart legal contracts may face challenges to ensure compliance in particular with the 14-day right of withdrawal, pre-contractual and other information requirements (e.g. the use of the language of code in code-only smart contracts may not fulfil the requirement of the contract terms being stated in a clear and comprehensible manner) and the mitigation of the effects of unfair contract terms. More specifically, for instance, challenges to comply with pre-contractual requirements are linked to the use of smart legal contracts that can be formulated exclusively in computer code language.[267] Challenges to comply with the right

[266] Oberlandesgericht München, Urteil vom 10.01.2019 - https://openjur.de/u/2297475.html.
[267] (forthcoming) Commission Study on Civil law rules applicable to smart contracts, p.80.

of withdrawal are due to the automatic and immutable nature of smart contracts on DLT, where a completed transaction may not be reversed.[268]

There are hardly any new EU rules specifically addressing aspects of automated contracting (aside from the Data Act i.e. Article 36(1)(b) on smart contracts for data sharing agreements) and no specific rules in B2C context. Under the AI Act, depending on the circumstances, typical consumer automation tools are likely to be qualified as low-risk AI systems, which would leave them subject to transparency obligations and voluntary codes of conduct.

The Data Act regulates enhanced[269] data access and sharing of co-generated IoT data and creates a data access right of the user (consumer or business) against the data holder (mostly the manufacturer or service provider) as regards products and related services data which were generated also because of the user using the product or related service. The user (e.g. a car buyer) can allow a third party (e.g. a repair shop or an insurance company) access to the data which this third party can request from the data holder. It is to be expected that the likely high number of data access requests especially via third parties will only be handled through automated, especially autonomous contracting and the use of smart contracts. In a B2C context, this would concern the contracts between data holders and consumers as users of connected products, e.g. cars.

In cases where the automation tools lead to damage, the consumer may seek compensation. In case the automated tool was an AI, different remedies are available. The victim may have a contractual liability claim if the defendant and the claimant have concluded a contract. In case the parties have not concluded a contract, the victim of damage caused by AI may have several non-contractual liability claims. In claims against any wrongdoer, the AI Liability Directive proposal may help consumers by easing the burden of proof in a targeted and proportionate manner using disclosure and rebuttable presumptions. This Directive would apply to all types of damages compensable under national law. In claims against producers, the Product Liability Directive enables consumers in the EU to claim compensation for material damage caused by a defective product. The revised PLD will cover both AI-enabled goods (as 'products') and AI systems on their own (as 'software'). However, compensation under the PLD will remain limited to proven or presumed defective AI and to damages resulting from death, or personal injury, or damage to, or destruction of, property and destruction or corruption of data that is not used for professional purposes. The right to compensation will cover all material losses resulting from the types of damage described above and non-material losses in so far as they are compensable under national law.

Taking the above into account, EU consumer law is currently not providing any specific protections to consumers that use such automation tools. Additional measures may be needed in the future to provide legal clarity and guidance to the market to ensure that consumers retain their freedom of choice and sufficient control as their transactional journey is increasingly automated.

[268] Ibid., p 91.
[269] To the extent personal data are concerned, the Data Act complements the right to access and port personal data under the GDPR.

VI.2. Other problems

The Fitness Check additionally analysed reports of other problems concerning specific business models, commercial practices and products. The main ones are highlighted below.

VI.2.1. Dropshipping

Dropshipping means the selling of products without their seller holding those products in stock. Where a consumer orders a product, the seller passes the order directly to the supplier (wholesaler or producer), who would subsequently take care of the logistics (direct delivery to consumer) and possible returns, without the need for the seller to be involved.

Responses to the public consultation highlighted some of the difficulties that EU consumers face in identifying where the traders are based, from where their products are shipped as well as the associated uncertainties regarding the protection of their consumer rights against non-EU traders. In the consumer survey conducted for this Fitness Check, 45% of consumers had experienced a situation where it was not made clear that the website/app where they purchased goods was acting as an intermediary which only transferred the details of their shipment to a different manufacturer or seller who was responsible for delivering their order. In the targeted survey, 72% of respondents found the absence of transparency about the dropshipping business model to be problematic.

Under EU consumer law, dropshipping is a legal selling method, provided that all the relevant consumer protection rules and other laws are complied with, such as giving the necessary pre-contractual information and ensuring that the products are safe. There have only been a few examples of enforcement actions and emerging national laws. In 2021, French authorities conducted an awareness campaign on scams identified in the dropshipping sector. The 2023 French influencer law imposed new responsibilities on influencers that make use of dropshipping and obligated them to inform consumers about the identity of the actual supplier and to ensure the availability and legality of the products, in particular that they are not counterfeit products.

The popularity of dropshipping in the EU may also be impacted by the recent changes resulting from the VAT e-commerce package. In particular, the VAT exemption for imports of small consignments of goods worth up to EUR 22 was abolished as from 1 July 2021 and there are new obligations concerning the distance sales of goods imported from third countries in consignments under EUR 150.

In the targeted survey, only 28% of respondents considered that EU consumer law provides regulatory certainty about dropshipping to a moderate or great extent and 57% of respondents supported further consideration of additional transparency requirements for those using a dropshipping business model. In view of these findings, it may be necessary to enhance transparency for consumers about this business model.

VI.2.2. AI chatbots

In the context of customer service, AI-powered chatbots can help traders communicate with consumers in a more efficient and targeted manner. However, the default or exclusive use of AI chatbots could hinder consumers from exercising their rights. Similarly to the dark patterns that create technical obstacles to contract cancellation or switching, the inability to contact a human interlocutor could undermine the effectiveness of EU consumer law. In the consumer survey conducted for this Fitness Check, 44% of consumers had experienced a situation where they found it difficult to resolve a problem with a company because they only had access to an automated chatbot and could not speak or

exchange messages with an employee. In the targeted survey, 64% of respondents agreed that traders communicating through AI chatbots is a concern. As a remedy, 65% of stakeholders responding to the public consultation called for the right to always have the possibility of contacting a human interlocutor upon request when AI chatbots are used to deal with consumer complaints and other inquiries.

At present, EU legislation, including the AI Act, does not contain such a consumer right for all B2C products. However, the AI Act ensures that for all high-risk AI systems there is a requirement for human oversight and that the persons concerned can also request an explanation about decisions taken on the basis of output from a high-risk AI system. In the area of financial services, in order to obtain adequate explanations, the recent review of the DMFSD introduced in the CRD a right to request and to obtain human intervention at the pre-contractual stage, and in justified cases after the distance contract has been concluded. The objective of this measure is to add transparency and provide the consumer with the right to request human intervention when he or she interacts with the trader through fully automated online interfaces, such as chatbots, roboadvice, interactive tools or similar means. Furthermore, the amended CCD introduced a right to human intervention where the creditworthiness assessment involves the use of automated processing of personal data (Art. 18(8)).

A more human-centred approach to AI chatbots in B2C customer service would be analogous to the modalities prescribed in the DSA, which clarified that there cannot be full automation concerning the single contact point established by providers of intermediary services (Art. 12) or concerning the decisions taken in the internal complaint-handling process by online platforms (Art. 20).

Furthermore, Art. 22 of the GDPR provides the right not to be subject solely to an automated decision-making that has legal or similarly significant effects, for example in the context of credit scoring. Such a prohibition does not apply when a data subject explicitly consents to be subject to such automated individual decision-making if it is necessary for the contract or authorised by Union or Member State law. In principle, when automated decision-making is allowed, the controller must provide for human intervention.

Against the background of the proliferation and advancement of AI chatbots in the customer service context, it may be necessary to take measures to preserve consumer choice and to enable consumers to exercise their rights effectively.

In terms of the application of the existing rules to AI chatbots, there are questions concerning the extent to which it is possible for AI chatbots, as an intermediary, to ensure compliance with certain consumer law obligations. For example, as consumers increasingly start to use AI chatbots as a search engine for product and service recommendations, it is likely that there will be sponsored content, advertorials or other commercial communications among the data that is used to compile an answer in response to the consumer's query. If traders providing the AI chatbot receive any payment for promoting the products or services of third parties, then they would have to ensure clear disclosure about this aspect, similarly to online marketplaces, search engines and product comparison sites. However, the situation is less clear in case there is no payment to the trader providing the AI chatbot. The impact of AI on search advertising and other stages of the consumer's transactional journey will have to be further monitored as the market develops.

VI.2.3. Scalper bots

Scalper bots are used to automatically purchase products in high demand with a view to reselling them at a higher price. As from 28 May 2022, the Modernisation Directive introduced in the UCPD a prohibition against the use of automated bots to scalp event tickets for reselling purposes when circumventing any limits imposed on the number of tickets that a person can buy or any other rules applicable to the purchase of tickets. However, media reports and consumer complaints have emerged about scalping practices in case of other products, such as gaming consoles, graphic cards and sneakers. In the targeted survey, only 27% of respondents considered EU consumer law to provide regulatory certainty to a moderate or great extent about the use of scalping.

With the exception of event tickets, the use of scalper bots is not directly regulated by EU consumer law. The UCPD could be used to tackle potentially deceptive practices; however, reselling through scalping is not *per se* illegal. Interviews with national authorities and consumer organisations highlighted some of the challenges concerning the regulation of scalping practices, such as defining the scope of scalping, determining permissible resale prices and practical enforcement difficulties given the cross-border nature of scalping activities. In the public consultation, 60% of stakeholders supported the further limitation of scalping for reselling purposes (42% strongly agreed, 19% agreed). The prevalence of the use of scalper bots for event tickets and other products should be further monitored to ascertain the extent of the consumer detriment.

VI.2.4. Ticket sales

The consultations highlighted concerns about the event ticket sector, in particular as regards dynamic pricing and ticket reselling practices.

Dynamic pricing refers to the changing of the price of a product in a highly flexible and quick manner in response to market demands. In July 2023, several MEPs requested the Commission to look further into dynamic pricing practices in the event ticket sector and to consider adopting additional legislative measures, such as requiring further transparency, establishing price ceilings or prohibiting the practice altogether.

Currently, dynamic pricing is not prohibited by EU consumer law. Traders can freely determine the prices they charge as long as they adequately inform consumers about the total price. However, commercial practices related to dynamic pricing could in some circumstances breach the UCPD, e.g. if prices are raised during the booking process after the consumer has proceeded to payment.

Concerning the problems with reselling, in the consumer survey, 33% of consumers had experienced a situation where they wanted to purchase a ticket for an event, but only saw tickets from secondary sellers available at a higher price. While the ban of event ticket scalping through the Modernisation Directive amendments to the UCPD and the requirement for indicating the status of the seller as a trader or a consumer were perceived as having a positive effect, several stakeholders highlighted problems that remain and suggested additional regulatory measures, such as obligating ticket resellers to disclose additional information (e.g. the original face value of the ticket, any additional fees or charges, and the seat location), setting limits on resale prices (e.g. no more than the original seller's price of the ticket or with a cap), requiring uncapped secondary ticket resale sites to make their status clear in search engine listings and the establishment of official platforms for ticket resale, controlled by event organizers or authorized entities, which could contribute to the availability of fair pricing and authentic tickets. In the public consultation, 53% of stakeholders supported mandating more specific information

obligations when products such as event tickets are sold in secondary markets (34% strongly agreed, 20% agreed).

In light of the above, the extent of the problems with dynamic pricing in the event ticket sector should be further monitored and it may be necessary to further enhance the transparency of practices regarding ticket reselling.

Digital Services Act[270]
General relationship with consumer law: Article 2(4)(f) - This Regulation is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing this Regulation, in particular, the following: (f) Union law on consumer protection and product safety, including Regulations (EU) 2017/2394 and (EU) 2019/1020 and Directives 2001/95/EC and 2013/11/EU
Article 6 DSA – Exemption of liability for hosting Article 6(1) provides that information society services that are hosting information shall not be liable for the information stored, subject to specific conditions. Article 6(3) clarifies that this exemption from liability shall not apply with respect to consumer protection law in situations where an online platform that enables consumers to conclude distance contracts with traders (online marketplace) presents information or otherwise enables the transaction in a way that would lead an average consumer to believe that such information or the product/service is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control. In addition, in line with Article 54 DSA, a provider of intermediary services is liable for any damages suffered by the recipients of the service caused by infringing of the obligations stemming out from the DSA, such as e.g. not acting upon notices.
Article 14 DSA – Terms and conditions Article 14 provides that intermediaries should include information on any restrictions regarding the use of their service in the T&Cs (e.g. policies and tools for content moderation). This information should be in "clear, plain, intelligible, user-friendly and unambiguous language" and publicly available in an easily accessible and machine-readable format. They also have to inform users of significant changes to the T&Cs. When the intermediary service is mainly directed at minors, T&Cs should be explained in a way that is understandable for minors. VLOPs and VLSEs have to provide a T&C summary and publish the T&C in all official languages of the Member States where they provide services.
Article 25 DSA – Online interface design and organisation Article 25 provides that 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

[270] 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).

service to make free and informed decisions'. However, this prohibition does not apply to 'practices covered by' the UCPD or GDPR.

It gives three examples of practices that could be regarded as dark patterns, while stipulating that the Commission may issue guidelines to further explain its application:

(a) giving more prominence to certain choices when asking the recipient of the service for a decision;
(b) repeatedly requesting that the recipient of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience;
(c) making the procedure for terminating a service more difficult than subscribing to it.

Article 26 and Article 39 DSA - Online advertising

Article 26 requires providers of online platforms to ensure that: advertising on their platforms is identifiable as such (including through prominent markings), that the person(s) on whose behalf the ad is presented and paid can be identified and that the main parameters for targeting recipients are presented.
Providers of online platforms also need to provide a functionality allowing users to declare whether the content they provide contains commercial communications.
The provision bans targeted advertising based on profiling that uses the special categories of personal data referred to in Article 9(1) GDPR.

Article 39 establishes the additional obligation for VLOPs and VLOSEs to compile and publish a repository with information about the advertisements displayed on the platform, to whom it was intended to be addressed etc.

Article 3(r) defines 'advertisement' as the promotion of information by the online platform on behalf of a legal or natural person against remuneration.

Article 27 and Article 38 DSA – Recommender systems

Article 27 requires providers of online platforms to provide, in their terms and conditions, the main parameters of recommender systems.
If several versions of the recommender system are available, a functionality needs to be provided that allows users to select and modify their preferred option.

Article 38 establishes an additional obligation for VLOPs and VLOSEs: they need to provide at least one option for each of their recommender systems that is not based on profiling (i.e. not personalised).

Articles 28, 14(3) and 34(1)(d) DSA - Protection of minors

Article 28 bans targeted advertising directed to minors. It also requires providers of online platforms to put in place appropriate and proportionate measures to ensure a safe service for minors. The Commission may issue guidelines on the subject.

Article 34(1)(d) lists actual or foreseeable negative effects in relation to minors as one of the systemic risks that VLOPs and VLOSEs are required to identify, analyse and assess.

Article 30 DSA – Traceability of traders

Article 30 requires marketplaces to vet the credentials of their online retailers before they list them ('Know-your-business-customer principle'). B2C platforms are required to store relevant information until six months after the end of the contractual relationship with the online retailer. Part of the information needs to be published on the platform (trader's name, address, telephone number and email address; information about its registration in a trader register or similar; self-certification committing to only offering products that comply with EU law). Under certain conditions, B2C platforms are required to refuse or suspend the listing of an online retailer.

Article 31 DSA – Compliance by design

Article 31 requires marketplaces to design and organise their online interface in a way enabling their online retailers to comply with their obligations regarding pre-contractual information as well as compliance and product safety information ('compliance by design'). Before listing online retailers, B2C platforms are required to make best efforts to assess whether the online retailer has provided relevant information. Article 31 also obligates B2C platforms to randomly check if the products or services offered by their online retailers are listed as illegal.

Article 32 DSA – Right to information (illegal products or services on marketplaces)

Article 32 requires marketplaces to inform consumers that an illegal product or service has been offered by a trader, including about the identity of the trader/seller and any relevant means of redress. Such information must be provided by contacting the consumers who bought such products or services directly or, in case they do not have the contact details, marketplaces must make such information publicly available on their online interface.

Articles 34 and 35 – Risk assessment and mitigation

Article 34 requires VLOPs and VLOSEs, on a yearly basis, to identify, analyse and assess any systemic risks stemming from the design or functioning of their service and its related systems or from the use made of their services. The systemic risks include any actual or foreseeable negative effects on the high level of consumer protection and the rights of the child.

Article 35 requires VLOPs and VLOSEs to put in place reasonable, proportionate and effective mitigation measures, tailored to those identified risks. Measures can include adaptations to their services, online interfaces, T&Cs, awareness-raising measures etc.

Article 44 DSA – Standards

Article 44 requires the Commission to consult the European Board for Digital Services and support and promote voluntary standards by European and international standardisation bodies in respect of several areas, such as:
(b) templates, design and process standards for communicating with the recipients of the service in a user-friendly manner on restrictions resulting from terms and conditions and changes thereto,
(h) technical measures to enable compliance with obligations related to advertising, (..) including the obligations regarding prominent markings for advertisements and commercial communications,
(i) choice interfaces and presentation of information on the main parameters of different types of recommender systems,

(j) standards for targeted measures to protect minors online.

Article 45 and Article 46 DSA – Codes of conduct

Article 45 requires the Commission and the Board to facilitate voluntary codes of conduct to enhance compliance with the DSA. They are required to assess the codes of conduct and regularly monitor and evaluate whether they achieve their objectives.

Article 46 establishes a similar obligation for the Commission with regard to voluntary codes of conduct to contribute to further transparency for actors in the online advertising value chain, beyond the requirements of Article 26 and 39.

Digital Markets Act[271]

General relationship with consumer law:
Recital 12 - This Regulation should apply without prejudice to the rules resulting from other acts of Union law regulating certain aspects of the provision of services covered by this Regulation, in particular (…) 2005/29/EC (…) 93/13/EEC, as well as national rules aimed at enforcing or implementing those Union legal acts.

Article 5 DMA – Obligations for gatekeepers

Article 5 establishes specific obligations for gatekeepers, which directly impact B2C services and consumer choice, including in the following cases:
5(2) – not allowed to process or combine personal data without the consumer's consent (when processing for online advertising purposes the personal data of users of third-party services that make use of gatekeeper's core platform services; combining data from core platform service with data from other gatekeeper or third party services; cross-using personal data across different gatekeeper services; signing in to other gatekeeper services to combine data);
5(3) – right for business users to offer consumers different prices and conditions when selling products or services through their own website compared to when selling them on a gatekeeper's intermediation service;
5(4) – right to receive commercial communications and conclude contracts with businesses outside of the gatekeeper's core platform services;
5(5) – right to access and use content, subscriptions, features or other items acquired without using a gatekeeper's core platform services, whilst using the software applications of a business through the gatekeeper's core platform services (e.g. an app store);
5(6) – no restriction of consumer's ability to raise issues of non-compliance by the gatekeeper with Union or national law with any relevant public authority;
5(7) – no requirement for consumers to use an identification service, web browser, payment service or related technical services of the gatekeeper, when using a third-party service that makes use of a gatekeeper's core platform service;
5(8) – no requirement for consumers to subscribe or register with further services as a condition for accessing the gatekeeper's core platform services.

Recitals 36-37 also explain that gatekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a 'less personalised but equivalent alternative', and without making the use of the core platform service or certain functionalities thereof conditional upon the end user's consent. The less

[271] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent.

Article 6 DMA – Obligations for gatekeepers susceptible of being further specified under Article 8

Article 6 establishes specific obligations for gatekeepers, which directly impact B2C services and consumer choice, including in the following cases:
6(3) – right to easily uninstall apps on the operating system of the gatekeeper and right to easily change default settings on the operating system, virtual assistant and web browser of the gatekeeper;
6(4) – right to install and effectively use new apps and app stores by third parties, including outside a gatekeeper's app store;
6(5) – no self-preferencing of the gatekeeper's products and services compared to third parties' products and services in ranking and related indexing and crawling;
6(6) – no restriction of switching between different apps and services that are accessed using the gatekeeper's core platform services;
6(7) – right to the same interoperability with the hardware and software features of a gatekeeper's operating system and virtual assistant, as enjoyed by the gatekeeper's own services and hardware;
6(9) – right to data portability concerning data provided or generated through the use of gatekeeper's core platform services;
6(13) – conditions for terminating core platform services cannot be disproportionate or exercised with undue difficulty.

Article 7 DMA – Obligations for gatekeepers on interoperability of number-independent interpersonal communications services

Article 7 introduces a new obligation for gatekeepers to provide for interoperability between their own messaging service and the messaging service of a provider that introduces a reasonable request, while ensuring the necessary level of security and end-to-end encryption that is provided by the gatekeeper to the consumers of its own services.

Article 13 DMA – Anti-circumvention

Article 13 prohibits gatekeepers from circumventing the obligations in the DMA through contractual, commercial, technical or any other means, which includes the use of dark patterns to unfairly steer consumer decisions. Gatekeepers are not allowed to degrade the conditions or quality of the core platform services to consumers who avail themselves of the rights or choices in Art 5-7 DMA, or to make the exercise of those rights unduly difficult, including by offering choices in a non-neutral manner or by subverting the consumer's autonomy, decision-making or free choice via the structure design, function or manner of operation of a user interface or a part thereof.

Article 15 DMA – Obligation of an audit of the report on consumer profiling techniques

Article 15 requires gatekeepers to conduct and submit to the Commission independently audited descriptions of any techniques for profiling of consumers applied in its core platform services and make an overview available to the public.

Data Act[272]
General relationship with consumer law: Article 1(9) - This Regulation complements and is without prejudice to Union law which aims to promote the interests of consumers and ensure a high level of consumer protection, and to protect their health, safety and economic interests, in particular Directives 93/13/EEC, 2005/29/EC and 2011/83/EU.
Article 3 – Obligation to make IoT product data and related service data accessible to the user Article 3(1) places an obligation on the manufacturer to design products and related services in a way that the user can access the data generated by their use. Article 3(2) and (3) prescribe pre-contractual information requirements as to how the user may access, retrieve or, where relevant, erase the data, including the technical means to do so, as well as their terms of use and to data collection and access under Art. 3(3). It includes information such as the duration of retention, whether the prospective data holder expects to use readily available data itself and the purposes for which those data are to be used, and whether it intends to allow one or more third parties to use the data for purposes agreed upon with the user and the identity of the prospective data holder, such as its trading name and the geographical address at which it is established and, where applicable, of other data processing parties.
Articles 4, 5 and 6 – Rights and obligations regarding IoT data access and sharing Article 4 outlines the conditions under which data holders should, on the basis of a simple request, make readily available data accessible to the user without undue delay easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. Article 4(4) and Article 6(2)(a) prohibit data holders from making the exercise of choices or rights more difficult through dark patterns (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 or the user). Article 5 gives the user the right to share such data with third parties. Article 6(2)(b) prohibits third parties that receive consumer data from connected products or related services from using that data for profiling unless it is necessary to provide the service requested by the user. Article 6(2)(h) prohibits third parties from preventing a user that is a consumer, including on the basis of a contract, from making the data they receive available to other parties.
Articles 23, 25, 29 and 30 - Switching data processing services (cloud providers) Article 23 prescribes several technical and non-technical obligations, including the removal of pre-commercial, commercial, technical, contractual and organisational obstacles, for providers of data processing services and prohibits them from imposing such obstacles, with the aim to enable consumers to switch between data processing

[272] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

service providers, or to change to on-premises ICT infrastructure, or, where relevant, use several providers of data processing services at the same time.

Article 25 requires the switching-related rights of the customer and the obligations of the provider of the data processing service to be laid down in a written contract and, without prejudice to the DCD, sets out the minimum content of this contract.

As of 11 January 2024, Article 29 requires providers of data processing services to reduce any remaining switching charges that are passed on to the customer to the costs that the provider incurs for switching. As of 12 January 2027, the Article prohibits switching charges. This includes charges for data egress. Article 29(4) requires data processing service providers to, prior to entering into a contract with the consumer, provide the consumer with clear information on standard service fees, early termination penalties and reduced switching charges.
Recital 89 highlights that early termination penalties must also remain proportionate. Such costs could amount to the contract value for the remainder of the term; however, they should not be used to penalize customers for switching providers. In addition, the Data Act places importance on maintaining the choice for consumers to conclude fixed-term contracts.
The Data Act lays down the minimum practices that providers will have to undertake to facilitate their customer's move to another provider. In this context, the Data Act distinguishes between providers of Infrastructure as a Service, for whom it introduces the concept of functional equivalence, and providers of Platform and Software as a Service, who are required to provide their customers with open interfaces and export data in a a structured, commonly used and machine-readable format.

Article 36 - Essential requirements regarding smart contracts for executing data sharing agreements

Article 36(1)(b) imposes an obligation on the provider of smart contract to ensure the existence of a mechanism allowing the safe termination and interruption of the smart contract.
Recital 104 explains that the use of smart contracts for the execution of data sharing agreements does not affect the application of existing consumer law to those agreements. In light of this, the essential requirement prescribed in Article 36(1)(b) is key to ensuring that, should certain terms of the data sharing agreement be considered unfair, the automated execution of the contract could be stopped.

AI Act[273]

General relationship with consumer law:
Article 2(9) – This Regulation is without prejudice to the rules laid down by other Union legal acts related to consumer protection and product safety.

Article 5 AI Act – prohibited AI practices

The following AI practices are prohibited and could be relevant in the B2C context:
(1) AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques with the objective to or the effect of materially distorting behaviour and cause or are likely to cause significant harm;

[273] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

(2) AI systems that exploit vulnerabilities based on age, disability or a specific social or economic situation of persons or a group of persons with the objective to or the effect of materially distorting their behaviour and cause or are reasonably likely to cause significant harm.

Article 6 and Annex III AI Act – high risk AI systems

The following AI systems are categorised as high risk and could be relevant in the B2C context:
- AI systems intended to be used as a safety component of a product, including that product, or if the AI system is itself a product covered by Union harmonisation legislation in Annex II;
- biometric categorisation according to sensitive or protected attributes or characteristics based on inference from such factors;
- emotion recognition;
- evaluating creditworthiness of natural persons or establishing their credit score (unless for detecting financial fraud);
- risk assessment and pricing in relation to natural persons in the case of life and health insurance.

AI systems are classified as high risk 'unless those systems do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making'.

The consequence of the high-risk categorisation is that the AI system would have to meet more stringent requirements, including in terms of risk management and documentation (**Articles 8-27 AI Act**).

The list of high risk systems could be expanded in the future via delegated acts to amend Annex III. The relevant factors in such an assessment would include for example the intended purpose of the AI system, the nature and amount of data processed and used by that AI system (in particular whether special categories of personal data are processed), the extent to which it has already caused harm or is likely to cause harm to the health and safety of persons, and the text to which there is an imbalance of power or the potentially harmed persons are in a vulnerable position.

Article 50 AI Act – transparency obligations for providers and users of certain AI systems

New information requirements that could be relevant in the B2C context:
- obligates providers of AI systems that are intended to directly interact with natural persons to be designed and developed in such a way that the persons are informed about the fact that they are interacting with an AI system (unless that is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use);
- obligates deployers of an emotion recognition system or a biometric categorisation system to inform natural persons that are exposed to it about its operation;
- obligates deployers of an AI system that can generate deepfakes to disclose that the content has been artificially generated or manipulated;
- obligates deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest to disclose that the text has been artificially generated or manipulated.

Article 86 AI Act – right to explanation of individual decision-making

Any affected person subject to a decision which is taken on the basis of the output from a high-risk AI system, which produces legal effects or similarly significantly affects them in an adverse way concerning their health, safety and fundamental rights, shall have the right to request from the deployer clear and meaningful explanations on the role of the AI system in the decision-making procedure and main elements of the decision taken.