



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

Final Report - Part 1

Lead author: Mark Whittle, CSES.

Contributing authors: Adam Humphreys, James Eager, Laura Granito, Rocio Salado (CSES), Laura Eid (CSES associate), Alessandra Innessi, Sose Mayilyan, Jan Demidovits-Mekeläinen, and Nessa Gorman (EY) and Cristina Poncibo (EY associate), Ninon Gautier, Julia Halej and Lugh Voarino, Tetra Tech, Quentin Liger, Asterisk, Ilsa Godlovitch and Peter Kroon (WIK), Charlotte Duke (LE Europe).

Legal academic reviewers: Prof. Mateja Durovic and Prof. Teresa Rodriguez De Las Heras Ballell

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

Final Report - Part 1

Notice

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

List of acronyms and glossary of terms	6
1 Study objectives and scope	8
1.1 Overview	8
1.2 Fitness Check introduction	8
1.2.1 EU policy context	8
1.2.2 Study objectives and scope.....	9
1.3 Methodology.....	13
1.4 Conceptual framework	16
1.4.1 Fitness for purpose of the legal architecture.....	17
1.4.2 Key concepts	18
1.4.3 Intervention logic.....	23
2 Problematic practices in the digital environment	31
2.1 Problematic practices	31
2.1.1 Overview of problematic practices in a fitness check context	31
2.1.2 Dark patterns	42
2.1.3 Aggressive practices.....	50
2.1.4 Subscriptions	53
2.1.5 Personalised advertising	62
2.1.6 Personalised pricing.....	68
2.1.7 Social commerce and influencer marketing.....	70
2.1.8 Digital addiction.....	75
2.1.9 Dropshipping.....	87
2.2 Summary - national legislation to address problematic practices	88
3 Assessment of the Fitness Check evaluation questions	93
3.1 Effectiveness	93
3.1.1 Progress towards general objectives.....	93
3.1.2 Progress towards specific objectives.....	95
3.1.3 Progress in achieving regulatory certainty.....	102
3.2 Efficiency	134
3.2.1 Overview of the methodology and summary of the results	135
3.2.2 Evolution in B2C digital markets and services and review of market size	137
3.2.3 Costs and benefits for traders	147
3.2.4 Costs and benefits for consumers	177
3.2.5 Costs and benefits for consumer protection authorities	197
3.2.6 Proportionality of costs and benefits.....	201
3.2.7 Opportunities for simplification	205
3.2.8 Summary assessment of the costs and benefits of EU consumer law in the digital environment for different stakeholders	207
3.3 Relevance	208
3.3.1 Relevance to identified needs	209
3.3.2 Relevance to addressing the needs of vulnerable consumers in a digital context	

3.3.3	Relevance of EU consumer law to new technological and/ or market-related developments	216
3.3.4	Overall fitness for purpose and extent of legal gaps.....	230
3.4	Coherence.....	268
3.4.1	Methodology for assessing internal and external coherence	269
3.4.2	Internal coherence	269
3.5	External coherence	282
3.5.1	Introduction.....	282
3.5.2	Digital Services Act.....	290
3.5.3	Digital Markets Act	299
3.5.4	AI Act.....	303
3.5.5	e-Commerce Directive	306
3.5.6	GDPR	307
3.5.7	e-Privacy Directive	309
3.5.8	Data Act.....	310
3.5.9	Audiovisual Media Services Directive.....	312
3.5.10	Fundamental rights and equalities legislation.....	313
3.5.11	Accessibility Act.....	314
3.5.12	Distance Marketing of Financial Services (DMFSD).....	315
3.5.13	General Product Safety Regulation (GPSR)	317
3.5.14	Thematic issues.....	318
3.5.15	Overall findings.....	328
3.6	EU added value.....	332
4	Summary of Fitness Check findings and conclusions	338
4.1	Overall findings.....	338
4.1.1	Effectiveness	338
4.1.2	Efficiency	340
4.1.3	Relevance.....	342
4.1.4	Coherence	343
4.1.5	EU added value	344
4.2	Recommendations	344
4.2.1	Regulatory measures.....	344
4.2.2	Strengthening enforcement and monitoring.....	347
4.2.3	Non-regulatory measures.....	348
4.2.4	Importance of a holistic approach to strengthening consumer protection in a digital fairness context.....	349

List of acronyms and glossary of terms

List of acronyms and key terms	Description of term and/ or meaning of acronym
ADR	Alternative Dispute Resolution
AI	Artificial intelligence
AIA	Artificial Intelligence Act
AVMSD	Audiovisual Media Services Directive 2010/13/EU as revised by Directive (EU) 2018/1808
B2B	Business-to-business
B2C	Business-to-consumer
BEUC	BEUC is the European Consumer Association and umbrella group for 45 independent consumer organisations from 31 countries.
BRG	Better Regulation Guidelines
CBA	Cost-benefit analysis
CPAs	Consumer Protection Authorities
CPC	Consumer Protection Cooperation (CPC) Network
CRD	Consumer Rights Directive 2011/83/EU
DG CNECT	Directorate General for Communications Networks, Content and Technology
DG GROW	Directorate General for the Internal Market, Industry, Entrepreneurship and SMEs
DG JUST	Directorate General for Justice and Consumers
DLT	Distributed Ledger Technology (DLT) is a decentralised database managed by multiple participants, across multiple nodes. Blockchain is a type of DLT where transactions are recorded with an immutable cryptographic signature called a hash.
DMA	Digital Markets Act
DMFSD	Distance Marketing of Financial Services Directive
DSA	Digital Services Act
DPA	Data Protection Authority
Dropshipping	Dropshipping is a way in which traders sell products online through e-commerce platforms and marketplaces without keeping them in stock.
DSPs	Digital services providers
ECCs	European Consumer Centres

List of acronyms and key terms	Description of term and/ or meaning of acronym
FMCG	Fast-moving consumer goods
GDPR	General Data Protection Regulation (EU) 2016/679
IoT	Internet of Things
MD	Modernisation Directive, Directive (EU) 2019/2161 (commonly known as the Omnibus Directive)
NACE	NACE is the “statistical classification of economic activities in the European Community”
PID	Price Indication Directive. Whilst not part of the fitness check scope, this was included within the Modernisation Directive amending legislation.
RoW	Right of Withdrawal – the 14-day cooling off period when a contract is first entered into, as legislated through the Consumer Rights Directive (which can be extended to 30 days for doorstep selling as a regulatory option for unsolicited sales only).
Scalper bots	A scalper bot is an automated tool that purchases services and products in bulk, such as events tickets or other goods in limited supply. These tools can complete checkout processes faster than humans.
SCM	Standard Cost Model
UCPD	Unfair Commercial Practices Directive 2005/29/EC.
UCTD	Unfair Contract Terms Directive 93/13/EEC.

1 Study objectives and scope

1.1 Overview

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*’ was carried out for DG Justice and Consumers (DG JUST) under Framework Contract JUST/2020/PR/03/0001. The study was led by the Centre for Strategy and Evaluation Services (CSES), supported by EY (lead on the application report on the Modernisation Directive), Tetra Tech and Asterisk. Further organisations supported the analysis in specialist areas (e.g. WIK covered personalised advertising and pricing and LE Europe integrated a behavioural economics dimension into the analysis of the consumer survey results).

1.2 Fitness Check introduction

1.2.1 EU policy context

Digital transition has been actively promoted since the start of the mandate of the Von der Leyen Commission in the 2019. It builds on the EU’s commitment to digitalisation as a driver of the single market (Commission Communication ‘A Digital Single Market Strategy for Europe of 6 May 2015’¹).

In the **New Consumer Agenda**² Communication of 13 November 2020, digital transformation is one of five key priority areas. All five key priority areas in the Agenda are relevant to assessing the fitness of the body of EU consumer law, but four are especially relevant: (i) The digital transformation; (ii) Redress and enforcement of consumer rights and (iii) Specific needs of certain consumer groups and (iv) International cooperation (given that digital markets and services are global). The Agenda stresses that “digital information could empower consumers to check the reliability of information, make comparisons between products, but also inform them in a more holistic way about their environmental impacts, for example their carbon footprint” (pg. 9). The New Consumer Agenda also saw the need to take action to address problematic practices: “*Commercial practices that disregard consumers’ right to make an informed choice, abuse their behavioural biases, or distort their decision-making processes, must be tackled. These practices include the use of ‘dark’ patterns, certain personalisation practices often based on profiling, hidden advertising, fraud, false or misleading information and manipulated consumer reviews*”. In action point 7 of the Agenda, the Commission announced its intention to analyse whether additional legislation or other action is needed in the medium-term to ensure equal fairness online and offline.

As a first step, in 2021 the Commission updated its guidance documents on the Unfair Commercial Practices Directive (UCPD) and Consumer Rights Directive (CRD) which tackle application issues and problematic digital practices, alongside the 2019 guidance on the Unfair Contract Terms (UCTD). In May 2022, the Commission launched a Fitness Check of EU consumer law on digital fairness, evaluating the UCPD, CRD and UCTD to assess whether the regulatory framework in EU consumer policy is fit for purpose. The aim is also to identify any overlaps, gaps, inconsistencies and/or obsolete measures which may have appeared over time in the legislation, and to consider any cumulative impacts. The extent to which the benefits are proportionate to the costs and / or whether there are any excessive administrative costs and burdens for economic operators and for Consumer Protection Authorities (CPAs)

¹ A Digital Single Market Strategy for Europe, COM/2015/0192 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192>

² Commission Communication of 13 November 2020 on the New Consumer Agenda - Strengthening consumer resilience for sustainable recovery (COM(2020) 696 final)

responsible for monitoring and enforcing the implementation of the legislation also requires consideration.

1.2.2 Study objectives and scope

The overarching study objective was to support the Commission's work on the Fitness Check to assess **digital fairness** in three key EU consumer Directives. The legal scope of the study focuses on:

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

The study provides the Commission with the evidence base needed to carry out a Fitness Check of EU consumer law on digital fairness in the digital environment. The purpose was to determine how far, given the rapid changes in the digital environment, EU consumer laws have ensured a continuing high level of consumer protection, considering both new technologies and digitalisation-driven developments. This was examined through an assessment of the application and ongoing fitness for purpose of the three above-mentioned Directives, considering relevant trends in digital markets and services and changes in the business models of traders within these markets, which have been constantly evolving.

Whilst no formal definition of digital fairness was provided, for the purposes of the study, this can be understood as the imperative of ensuring that the fairness principle inherent in consumer law generally (and in the UCPD and UCTD explicitly) that consumers are long accustomed to in the offline environment should extend to digital markets and services given the technology-neutral nature of the legislation.

While an important **Fitness check of EU consumer and marketing law**³ was undertaken for DG JUST in 2017 which synthesised the results of a series of studies and evaluations across the body of EU legislation, the previous study assessed the fitness for purpose of the law applied both offline and online, with a consideration of whether there remained any cross-border obstacles to trade. The earlier study focused on a broader range of issues around the fitness for purpose of the EU consumer law acquis and included wider consumer and marketing law. For instance, a Business to Business (B2B) instrument, the Misleading and Comparative Advertising Directive, was included, but this is not part of this study's scope, whose scope was solely Business to Consumer (B2C) focused legislation.

Although EU consumer law's application in the digital environment was covered to some extent in the earlier study, this area has developed markedly since that time. There have been **major developments in digital markets and services**, such as the growth in the platform and subscription economy, rapid digital transformation of traders, and corresponding developments in business practices. Additionally, there have been **technological developments within the broad context of digitalisation and digital transition** that require examination in terms of their implications for the ongoing fitness for purpose of consumer law, such as Artificial Intelligence and the growing role of algorithms in personalisation (e.g. of advertising, pricing), product connectivity and the Internet of Things (IoT).

In terms of legislative changes, the **Modernisation Directive (EU) 2019/2161 (MD)** – also known as the '**Omnibus**' Directive – amended existing directives for the improved enforcement and modernisation of EU consumer protection rules. A separate report has been produced on the Modernisation Directive's transposition and application, although some references to the MD's role and the potential differences this amending legislation can make

³ Study for the Fitness Check of EU consumer and marketing law
<https://op.europa.eu/en/publication-detail/-/publication/f7b3958b-772b-11e7-b2f2-01aa75ed71a1/language-en>

are included within the fitness check report, since some changes are relevant to digitalisation and to strengthening enforcement, which both impact on digital fairness. The MD, for instance, directly amended the three pieces of legislation within the scope of the fitness check, as well as the Price Indication Directive (PID) underlining its relevance. Some of the regulatory changes pertain to the digital area, such as the prohibiting of fake online reviews and scalper bots for event tickets, and the strengthened transparency requirements for online platforms. The MD also sought to strengthen enforcement through regulatory amendments that harmonise penalties. These regulatory changes were a response to one of the limitations in the effectiveness of the application of EU consumer legislation under review identified in the previous Fitness Check, but also in other underlying studies undertaken in 2016-17, including the *Evaluation of the Consumer Rights Directive*. It could be argued that changes to penalties to make them more harmonised are especially relevant to the digital environment given that traders such as online platforms and marketplaces often operate on a pan-European and global basis. Some EU consumer law instruments (e.g. the UCPD, UCTD) make use of a **general principles-based approach** where traders need to avoid consumer harm by applying a principles-based test while the general clauses of these Directives are used to assess the unfairness of commercial practices and contract terms on a case-by-case basis. The study explored how far the general principles-based approach has been effective, applied in conjunction with **technology neutrality** as a key principle underpinning the legal framework's application.

A further study consideration was that there has been a **significant evolution in digital law and in broader EU legislation applicable to traders in the digital environment**. Therefore, with the rapid evolution of the interacting regulatory, technological and market elements, it was appropriate to consider the current fitness for purpose of EU consumer law, recognising that relevance may change over time depending on the nature of the new legal, technological, and market-related developments.

There has been a **trend towards the development of more specific rules regulating (and/or prohibiting) certain business practices in the digital environment** in some Member States (MS) and in some third countries too. This raises issues regarding the operation of the digital single market, given the risk of regulatory fragmentation if some MS regulate certain business practices deemed problematic, such as subscription traps, influencer marketing, loot boxes, and access to social media to protect children, while others rely on the general principles-based provisions of the UCPD and UCTD.

The **development of national rules in some countries** also raises considerations at EU level regarding what is the **optimal regulatory approach to ensure digital fairness**, including the appropriate balance between a general principles-based approach and more specific rules where appropriate, whilst maintaining technology neutrality.

The present fitness check provides an **in-depth empirical investigation of the ongoing fitness for purpose of the legislation to accommodate digital-related developments**, whilst recognising the legal framework seeks to ensure high levels of consumer protection through a general principles-based approach which is **applicable to traders in both the offline and online environment**.

The issue of the implementation of EU consumer law in a digital context in the light of changing digital technologies was partially considered in the 2017 fitness check. However, the **specific concept of 'digital fairness' and how far this has been achieved through the application of existing EU consumer law**, has only been analysed during this study. Since the time of the earlier fitness check, there has been a shift in the policy discourse among relevant stakeholders which has focused on the topic of digital fairness and whether **new and emerging 'digital asymmetries' experienced by consumers** have led to changes in traditional asymmetrical relationships between consumers and traders. Section 1.4 highlights the concept of digital asymmetries which are pervasive in digital markets and services and explains the need to ensure digital fairness. The extent to which key concepts such as an

‘**average consumer**’ and a ‘**vulnerable consumer**’ remain relevant in the digital environment and how far – if at all – this requires any aspects of the consumer law legal framework to be reviewed and possibly updated in future is also considered.

In summary, the overarching aim of the Fitness Check is to determine how far EU consumer legislation - specifically the UCPD, CRD and UCTD - have ensured a high level of consumer protection in the digital environment, in the light of developments in new technologies, the role of digitalisation in accelerating the growth and development of new digital markets and services, and whether these developments raise any regulatory considerations, including the nature and extent of any legal gaps. The findings will serve as the basis for drawing policy conclusions from the assessment of the fitness for purpose and relevance of the EU consumer law framework in the digital context.

An assessment of the current application of the three consumer law Directives in scope was undertaken covering the different evaluation criteria highlighted in the Better Regulation guidelines, namely **effectiveness, efficiency, relevance (including fitness for purpose), coherence** and **EU added value**. A detailed evaluation framework has been developed, but it is worth initially summarising what these criteria mean in practice in the context of this study:

Box 1-Error! Bookmark not defined. - Evaluation framework – simplified overview

- **Effectiveness:** What progress has been made towards the achievement of the (general, specific) objectives of the three pieces of EU consumer law within scope? Has the implementation of EU consumer law strengthened digital fairness more broadly? Has the regulatory architecture been effective e.g. in adopting a general principles-based approach or would more specific rules in certain areas have been more effective in addressing problematic practices?
- **Efficiency:** How far has the implementation of EU consumer law across the relevant Directives achieved an acceptable relationship between benefits and costs? How far was digital fairness achieved in an efficient manner? Were there any disproportionate administrative costs and burdens for traders and for enforcement authorities? What were the benefits for consumers and the disbenefits of ongoing consumer detriment due to the persistence of problematic practices?
- **Relevance (including fitness for purpose):** Has the EU consumer law framework remained relevant to identified needs? How far does it remain fit for purpose given technological, market-driven, and regulatory developments? Are more specific rules needed to address problematic practices or would this compromise technology-neutrality? Are there also complementary non-regulatory means of ensuring digital fairness?
- **Coherence:** Are the core legal texts and supporting guidance sufficiently clear? Is there evidence of any legal gaps between EU consumer law and other relevant EU legislation?
- **EU added value:** What would be the situation in the absence of EU consumer law in terms of ensuring digital fairness?

It was necessary to assess the ongoing relevance and coherence of EU consumer legislation given the rapid evolution in the overall body of relevant EU legislation. The **external coherence of EU consumer law within the broader EU legal framework** has been considered in the context of the increasing digitalisation of the European (and global) economy. There is growing complexity due to the gradual expansion of applicable EU laws, such as data and digital laws alongside EU consumer law relevant to traders in the digital environment. This has led to an increasingly complex inter-relationship between the application of EU consumer legislation and the requirement for the parallel application of consumer law based on other types of EU law. This is especially pertinent in the context of trends in digital markets and services, such as the growth in the data economy where transactions are often data-paid rather than involve monetary exchanges.

Beyond core consumer protection legislation and sectoral rules, the regulatory landscape includes digital-related legislation such as the Digital Services Act ('DSA'), Digital Markets Act ('DMA'), Artificial Intelligence Act ('AIA'), and data-related legislation, including the GDPR and the Data Act.

Parallel updates of sector-specific consumer protection laws should also be highlighted, as some of these have implications for consumer law. In recent years, relevant legal acts were updated to ensure that they are fit for purpose in the digital age. Examples are:

- **Protecting consumers in financial services contracts concluded at a distance.** On 28 November 2023, Directive (EU) 2023/2673 as regards financial services contracts concluded at a distance was adopted.⁴ This resulted in the Commission amending the Consumer Rights Directive to allow consumers to exercise their Right of Withdrawal (RoW) through the requirement that traders must provide a prominent withdrawal button.⁵⁶
- **Consumer Credit Directive (EU) 2023/2225⁷** updated the 2008 predecessor Directive to reflect rapid technological developments since its adoption which led to significant changes to the consumer credit market, both on the supply and demand sides, such as the emergence of new products and the evolution of consumer behaviour and preferences.

A mapping of relevant EU laws that impact on EU consumer law is provided in the section on external coherence. This provides a detailed assessment of relevant provisions across EU digital laws, EU data laws and other laws, including those that are sectoral, and whether there are any regulatory gaps for consumer protection. The effects of regulatory developments, including the updating of existing and the adoption of new EU legislation on the ongoing fitness for purpose of EU consumer legislation in the digital age raises strategic considerations. Examples are:

- How can EU consumer law be applied in parallel with multiple other pieces of law given the increased interconnectedness of such laws? For example, the DSA addresses dark patterns directly, whereas the UCPD covers dark patterns, but without explicit provisions. There is also increased importance of data in the digital economy which means that the GDPR is applied in close conjunction with EU consumer law, but with some ambiguities as to how this should be implemented e.g. there are rules on sensitive data in the GDPR, but a lack of any provisions on the use of such data in personalised ads in the UCPD, unlike for the more recent DSA.
- How to optimise the EU consumer law framework to strengthen consumer protection in the digital environment? Whereas the UCPD and UCTD are centred on a general principles-based approach, recent legislation on digital markets and services has introduced more specific rules. This raises a question as to whether some business practices and/ or some types of traders need specific rules from the consumer protection perspective, or whether the existing legal framework is already sufficiently clear in prohibiting certain practices. For example, hidden advertising prohibitions are covered in the UCPD, but influencer marketing poses challenges, with evidence of

⁴ European Commission, DIRECTIVE (EU) 2023/2673 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023L2673>

⁵ A withdrawal button will now be required for all digital products and services. Moreover, consumers will have the right to request human interventions on sites that display automatic information tools such as chatbots. Consumers have 14-calendar days to withdraw, but 30 days in case of personal pension operations. "Additional protection regarding online interfaces" was provided in that traders must not design online interfaces in a way that deceives or manipulates consumers.

⁶ Member States must address at least one of three practices: giving more prominence for certain choices, repeatedly asking consumers to make a choice, making the termination more difficult than subscribing to it.

⁷ DIRECTIVE (EU) 2023/2225 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC

insufficient disclosures on some platforms, and low compliance by influencers.

The fitness check is mostly **retrospective** in focus, but it is also **forward-looking** in examining the relevance criterion and when assessing problematic practices and possible solutions. To this extent, the ongoing fitness for purpose of the legislation has been assessed. The role of supporting (non-legally binding) guidance documents on each Directive to facilitate the application of the legislation has also been considered.

The study's main **geographical scope** covered the EU-27 Member States. However, in reviewing possible legal gaps in relation to new and emerging problematic practices, the research has included an international dimension where appropriate, for instance to ascertain how far particular practices have been regulated in other countries and/ or tackled through soft law measures.

The study focused on the **period** since the previous fitness check of EU law was undertaken in 2017 but also considers the whole period since the adoption of the three Directives. The precise timeframe considered therefore varied between the three Directives, given that the UCTD was adopted in 1993, the UCPD in 2005 and the CRD in 2011.

1.3 Methodology

The Fitness Check study was carried out over three Tasks. In summary:

- **Task 1 – Information gathering and analysis** – Collect data through five different consultations (a call for evidence, public consultation, targeted survey, consumer and enterprise survey), market analyses, sweeps of websites, desk research on digital business-to-consumer (B2C) practices identified as being potentially problematic.
- **Task 2 – Perform evaluation and fitness check** – Analyse the intervention logic underlying the three Directives, and consider any methodological and data / information limitations. Assess the evaluation questions (EQ) across the different criteria: **effectiveness, efficiency, coherence, relevance, and EU added value** and analyse a series of research questions (RQ). A list of EQ and RQ is in Annex 1.
- **Task 3 – Develop findings and conclusions** – Outline the study findings and conclusions by evaluation criterion.

The following assessment was carried out:

- Market developments and trends in digital business-to-consumer (B2C) practices within digital markets and services were analysed;
- The extent to which there are any specific problems in the application of EU consumer law Directives in the digital area was assessed. The analysis considered any general challenges, and the impact of the interaction between EU consumer law and the adoption of new, and updating of existing legislation (e.g. digital laws, data laws);
- The efficiency and effectiveness of the existing rules in addressing the problems identified was considered; and
- Possible means of addressing problematic practices were analysed. Regulatory and non-legislative solutions that could address these problems were identified. However, it should be recalled that this study is a fitness check. Potential regulatory solutions to obstacles would need to be further explored through an impact assessment.

The methodology was centred on a mixed methods approach combining interviews, several online surveys and extensive desk research. Whilst stakeholder feedback has been integrated into the main report, given the diverse methods and their extensive nature, and the need to answer the specific evaluation questions, the detailed results of the stakeholder consultations

are provided in a separate standalone annex. The methodology for the cost-benefit analysis (CBA) is explained in further detail in Annex 7.

In summary, the primary and secondary data collection activities undertaken were:

- **Interview programme** – 101 interviews were conducted in total. An overview of the interviews completed by type of stakeholder can be seen in the following table:

Table 1-1 - Interview programme - overview

Category of interviewee	Completed
Consumer association	13
EU policy maker	3
Legal researchers & academics	19
National enforcement authorities	4
National Ministries	30
NGOs	1
Online marketplaces	3
Online platforms	2
Software / search engines/ app producers/ AI developers	2
Traders	4
Trader associations (representing different industries e.g. digital-focused, sectoral associations, doorstep selling)	19
Total	101

- The interview programme achieved a balance between interviews linked to the fitness check and those focused on the application of the MD. A variety of stakeholders were interviewed for the fitness check e.g. Ministries, CPAs, consumer associations, trader associations, individual traders, online platforms and marketplaces and legal academics (covering both consumer law and digital and tech law specialisms).
- For the application check on the MD, all Ministries (except SK) were interviewed regarding their opinions and the assessment of the Modernisation Directive's transposition. These discussions also partially covered the fitness check including the issue as to how far the MD has addressed any gaps in EU consumer law in relation to ensuring fitness for purpose in the digital age. In addition, some Ministries (e.g. in Austria, Denmark, Germany and Italy) and CPAs participated in in-depth interviews when contributing to the digital fairness fitness check part. Fitness check interviews with different types of stakeholders (especially Ministries, trader associations, individual traders, including platforms) also covered issues relevant to the difference that the MD will make to achieving digital fairness for consumers.
- **Desk research** – an extensive literature review which included: (1) review of academic literature, such as research papers and studies on different aspects of the EU consumer law framework in the digital age; (2) legal research and analysis to review legal texts in respect of EU consumer law and guidance documents, and an assessment of external coherence between consumer law and other EU legislation, a review of national legislation relating to the transposition of the Modernisation Directive, etc.
- **Online Surveys and position papers** – input was received in particular from: (1) Call

for Evidence with 71 responses, (2) Public Consultation with 350 responses and 71 position papers - a factual summary report was produced and published based on the findings⁸, (3) Targeted Survey with 164 responses (4) Enterprise Survey of 1000 enterprises in representative sample of 10 MS and (5) Consumer Survey sample of 10,000 consumers in 10 MS. The findings of the surveys are set out in Annex 6, with key data and findings integrated into the main report.

- **Website/app sweeps** – sweeps were carried out to assess the extent of compliance among traders with existing rules and to check how far there may be additional problematic practices in specific areas. The topics covered were: telephone calls at basic rate, transparency of rankings of search results, personalised pricing and online consumer reviews, manipulative or opaque personalisation practices, digital subscriptions, transparency on online marketplaces, video games, price reductions and other types of price promotions, and customer service. The full sweeps are set out in the Annex. The main findings have been integrated into the main report.
- **Case studies** – eight case studies were developed (see Annex 5). These reviewed business practices considered to be problematic based on previous studies and evaluations. The assessment of problematic practices considered both longstanding challenges and new and emerging issues linked to practices in digital markets and services. The topics covered were: Unfair contract terms; Aggressive practices, Consumer vulnerability; Online subscriptions; Personalised advertising; Personalised pricing and offers; Digital addiction; and Social commerce and influencer marketing.
- **Part 1 – fitness for purpose of the EU consumer law framework.** The report assesses the evaluation questions, which address the fitness for purpose of the UCPD, CRD and UCTD. Practices considered to be potentially problematic are analysed in the main report under effectiveness and relevance, but explored in-depth in the supporting case studies (Annex 5).
- **Part 2 – review of national transposition of certain aspects of the Modernisation Directive.** Country fiches in Excel were developed for 26 out of 27 Member States. Only Slovakia is remaining where a draft law had been prepared but not yet been adopted during the writing of this report. 28 Ministries were interviewed since in some MS more than one interview was undertaken, reflecting different responsibilities for different pieces of EU consumer law, different individuals responsible for transposition vs. fitness check and policy-related matters pertaining to the Modernisation Directive.
- **Triangulation of information and data sources** – the analysis is based on extensive triangulation, for instance, cross-checking the interview notes with findings from the various online surveys and aligning with the results of the sweeps.

In the fitness check evaluation, a distinction has been made between:

- **Evaluation questions (EQs)** – the study addresses the EQs from the Tender Specifications in a streamlined way organised by evaluation criterion, covering effectiveness, efficiency, relevance, coherence and EU added value.
- **Research questions (RQs)** – a more specific set of issues, mostly linked to problematic practices. RQs are partly explored in the main report but also in the case studies focused on practices in areas such as subscription traps, aggressive practices, practices linked to the problem of digital addiction. Some of the most crucial RQs linked to problematic practices are also highlighted in the main report. It should be noted that the evidence presented on RQs is less detailed in terms of stakeholder feedback given

⁸ Factual summary – public consultation on the Fitness Check of EU consumer law on digital fairness (Ares(2023)2578495) - <https://ec.europa.eu/info/law/better-regulation/> and also see https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/public-consultation_en

the large number of EQs and the fact that the RQs are presented in detail drawing on extensive consultations and desk research in the case studies.

In Annex 1, a list of evaluation questions is provided covering the five key evaluation criteria specified in the Better Regulation Guidelines (BRG) and the additional research questions addressed in the study. This should be consulted by readers of the report as it signposts to where in the report and annexes particular topics and issues are covered.

1.4 Conceptual framework

The conceptual framework has been designed to consider the following:

- **The fitness for purpose of EU consumer law.** The current legal architecture and approach to the development and revision of EU consumer law was considered. The extent to which the general principles-based approach in the UCPD and UCTD described in Section 1.2 as a regulatory approach remains fit for purpose or whether more specific rules could be needed has been assessed in the context of the increased digitalisation and problematic commercial practices in certain areas of digital markets and services. The role and ongoing relevance of a technology-neutral approach in the design and updating of EU consumer law to ensure fitness for purpose was also considered.
- **The extent to which the mechanisms to strengthen the effectiveness of the UCTD, UCPD and CRD's application, and to maintain fitness for purpose are working well.** Examples include:
 - The Modernisation Directive's role in strengthening rules in the digital environment through regulatory amendments to the three Directives. Some of these address digital aspects (e.g. various information requirements for online platforms to strengthen transparency, prohibiting fake reviews), whereas others were non-digitally focused.
 - The role of national case law and CJEU rulings in clarifying the meaning of EU consumer legislation transposed into national laws (given the three pieces of law under review are all Directives), and ensuring legal clarity over time. A further consideration is whether the evolution in case law to reflect new and emerging business practices identified as unfair and therefore illegal under the UCPD and UCTD is sufficiently timely to ensure sufficient regulatory certainty for traders and consumers.
 - The interplay between EU consumer law and the supporting interpretative guidance documents. The guidance is acknowledged as being very useful by all stakeholders. However, there is an issue as to how detailed and specific the legislation itself should be and whether some aspects of the detailed guidance could be made more explicit in the legislative provisions (or at least the recitals).
- **The nature and extent of practices deemed problematic in the digital environment.** The analysis considers how far these practices are already prohibited in EU consumer law (and whether addressed implicitly or explicitly), and whether there are new and emerging practices where there is currently no legal protection. Possible legal gaps and/ or areas where regulatory uncertainty may arise are identified. A further consideration is whether there is a consensus among stakeholders that business practices are problematic in the first place. Whereas both traders and consumer representatives agree that some practices such as hidden advertising should be illegal, there are different opinions regarding other practices (e.g. what types of personal data should be allowed to target ads used in personalised advertising, etc.).

1.4.1 Fitness for purpose of the legal architecture

The overall fitness for purpose of the legal architecture underlying the EU consumer law framework within scope should be considered. The UCPD and UCTD are longstanding key pieces of EU consumer law. These include core provisions of a principle-based nature to ensure that traders' commercial practices and contract terms in consumer contracts are not unfair. Practices and contract terms would need to be assessed on a case-by-case basis to establish whether there has been a breach of specific consumer protection provisions. One of the benefits of a general principles-based approach is that case law plays a strong role in clarifying the meaning and application of the law over time. This retains flexibility in the system as the legal framework's application can evolve over time and cover new and emerging problematic practices. However, the disadvantages are that it may take extensive time for case law to emerge in response to new, problematic digital practices, causing legal uncertainty. Legal academics have estimated that the period between a problematic practice being identified and relevant case law emerging may be circa 5 years or more (by which time the practice may have changed, and/ or new problematic practices may have arisen).

Moreover, such case law may be confined to a limited number of Member States leading to over-reliance on one or two countries to provide most of the case law. A further disadvantage is that rules for the digital environment risk being insufficiently clear to ensure high levels of protection for consumers. As will be shown in Section 3.5 which considers external coherence between EU consumer law and other relevant legislation, there may be legal gaps from the existence of more detailed rules in some areas of EU law (e.g. dark patterns) compared with EU consumer law, where the general principles-based approach lacks specific rules to address specific problematic practices in some instances.

The EU consumer law framework is centred on the principle of **technology-neutrality**. According to stakeholders interviewed, an advantage of this regulatory approach is that the **legislation is applicable in both the online and offline environments**, thus maximising consumer protection, whilst allowing traders to follow a common set of rules irrespective as to whether their business model is mainly offline, online, or multi-channel. However, a disadvantage is that there are several digitalisation and technology-related developments that may require more specific and / or detailed rules than currently exist in EU consumer law. Indeed, as will be shown under the assessment of relevance and fitness for purpose (Section 3.3) and Coherence (Section 3.5), whilst the general principles-based approach is strongly appreciated by all stakeholders (especially traders and their representative associations, but also recognised as being valuable by consumer associations and CPAs), regulators globally have already introduced, or are considering introducing in future, some new rules on specific business practices across digital markets and services that are considered to be problematic.

Examples are the UK and US, as well as EU-27 MS such as **Germany** and **France**, introducing more specific rules on online subscriptions. Whereas there could be regulatory risks in regulating each specific business practice (not least, the fact that new business practices in digital markets and services evolve regularly), equally, consideration is needed in the study as to whether more the lack of specific rules for digital business practices is a problem.

It is worth noting that the European Commission's latest interpretative guidance documents (CRD, UCPD) already include updated examples of how to apply the legislation in the digital environment. For instance, Section 4.2 of the UCPD Guidance document focuses on the digital sector. It addresses issues such as online platforms and their commercial practices, the transparency of search results, data-driven practices and dark patterns and influencer marketing. It makes clear what is prohibited already under the UCPD. However, the guidance is not legally binding and only some traders (and their representative associations) look at the guidance and have familiarity with the detailed examples and supporting case law provided.

This raises an issue as to whether the legislation needs to be updated to provide an adequate regulatory response or if the guidance is sufficient.

When considering the legal architecture, it will also be important to analyse the fitness for purpose of EU legislation and soft law mechanisms that allow the UCTD, the UCPD and the CRD to be updated and to strengthen the effectiveness of their application over time. The legislation nonetheless continues to evolve, even if the general principles and most important requirements for traders remain broadly unchanged. Examples of developments relevant to improving the effectiveness and relevance of the Directives that demonstrate how EU consumer law evolves over time are summarised in the following typology:

Table 1-2 – Typology – changes to the legal framework, its interpretation and application

Types of changes over time	Examples
<p>Regulatory amendments to the underlying legislation CRD, UCPD and UCTD</p>	<ul style="list-style-type: none"> • The MD made some legislative amendments to the underlying Directives. Some of these regulated specific aspects of digital fairness. Enforcement was also strengthened through harmonised rules on penalties, with the potential to deter non-compliance by traders in the digital environment; • The DMFSD was repealed and integrated into the CRD, thereby expanding the CRD’s scope to financial services. It will introduce a right of withdrawal functionality (e.g. button) in the CRD to withdraw from all distance contracts and regulates certain dark patterns in the case of financial services contracts.
<p>Regulatory interpretation by the CJEU and national courts</p>	<ul style="list-style-type: none"> • Role of CJEU rulings and national case law in progressively clarifying the detailed application and implementation of EU consumer legislation over time. Through the general fairness test, case law plays a role in determining the interpretation of EU consumer law rules in relation to emerging business practices, some of which may be identified as problematic from a consumer protection perspective.
<p>Soft law mechanisms</p>	<ul style="list-style-type: none"> • The supporting interpretative Guidance documents by the Commission on the UCPD⁹ (2021); the CRD¹⁰ (2021); on the UCTD¹¹ (2019), 2021 Guidance on the PID, Art.6a; • National guidance documents on EU consumer law and their interpretation e.g. the Dutch ACM guidance on online persuasion; • CPC network initiatives to monitor levels of compliance and to strengthen enforcement; and • Other ad hoc initiatives, such as promoting industry self-regulation, EU and national government initiatives to strengthen awareness about current law and information obligations for traders to help increase compliance.

1.4.2 Key concepts

This section outlines key concepts relevant to assessing the ongoing fitness for purpose of

⁹ Guidance on the Unfair Commercial Practices Directive (2021) https://commission.europa.eu/document/download/4f3285e1-54ed-402f-a9a7-d6769240b1aa_en

¹⁰ Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021XC1229\(04\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021XC1229(04))

¹¹ Guidance on the Unfair Contract Terms Directive (2019) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2019.323.01.0004.01.ENG&toc=OJ:C:2019:323:TOC

the EU consumer law framework.

1.4.2.1 Digital fairness, informational and digital asymmetries

Digital fairness is not explicitly defined in the current EU consumer law framework. However, this emerging concept has attracted increased attention from regulators, consumer associations, legal academics and other stakeholders, including platforms and marketplaces both in the EU and globally. Digital fairness encompasses legal, informational and structural asymmetries, ethical and technical dimensions (for the latter, examples are dark patterns in online choice architectures).

There have been some attempts to define what digital fairness means. For instance, according to DIGITALEUROPE, “*digital fairness in EU consumer law involves ensuring that consumers are adequately protected in the digital realm. It aims to maintain trust by addressing potential gaps and challenges related to consumer rights online*”.¹² BEUC points to digital fairness being concerned with ensuring that whilst recognising the many benefits of digitalisation, consumers should not be put in a position of increased weakness. “*Digital companies control what we see and the choices we are given. They influence our experiences and decisions in ways that are far too complex to be understood by the average consumer. This complexity and increased business power requires a new approach to consumer protection, to strengthen consumer rights and redefine what fairness means in the new digital reality*”.¹³

Before considering the legal norms of an ‘average consumer’ and a ‘vulnerable consumer’, it is important to consider how the experience of consumers in the digital environment differs from traditional notions of consumer-trader informational imbalances.

Box 1-1 - Consumers in the digital environment

What does a consumer in the digital environment look like?

Consumers in the digital environment have several distinctive characteristics compared to those in traditional offline settings. It could be argued that there are push-pull factors which mean that consumers have greater choice in the digital environment in some instances, but reduced choices in others. For instance, consumers can access a vast array of information about products and services easily online theoretically, although their **choices may sometimes be limited due to dark patterns in interface design architectures**. Moreover, there is an interaction with competition law, as some intermediaries and platforms have a dominant market position, which may risk limiting consumers choices when considered in parallel with dark patterns.

Given the increased in transparency requirements, and the lengthy nature of terms and conditions, many consumers in the digital environment may perceive information overload, which can exacerbate asymmetries.

Today’s European digital consumer often expects a high level (or least some degree) of **personalisation and customisation of their online experiences**, whether relating to product recommendations or to targeted advertisements. However, consumers are often concerned about their privacy, given that they often relinquish large amounts of personal data in order to have personalised experiences.

Digital consumers - as in the offline environment - continue to expect fairness. Compared with the offline world, consumers are likely to be more **interactive in engaging with traders**, for instance through social media, websites, and apps. Moreover, they are likely to be **influenced by user-generated content**, such as ratings and reviews, as well as social media posts. These factors may influence their purchasing decisions, therefore it

¹² [Ensuring digital fairness in EU consumer law: taking stock of existing rules - DIGITALEUROPE](#)

¹³ https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf

is important they are not misleading or deceptive.

Digital consumers **require transparency and make transactional decisions based on trust**. They seek transparency by traders, and trust may be eroded by any unfair practices, and / of influenced by negative reviews from other consumers or service users. Regarding the **enforcement of rights for digital consumers**, consumers are more likely to face challenges. The global nature of digital transactions complicates enforcement of consumer rights and avenues for redress (e.g. when dealing with international traders/ sellers).

The digital consumer may have greater access to information (and in greater volume) than ever before. However, they **still experience deep structural asymmetries**, given the widespread use by websites and platforms of AI, including **algorithmic prediction technologies and machine learning to establish consumer preferences, influence decision-making and facilitate personalisation**. Whilst this benefits consumers, such practices sometimes raise fairness issues and it has become due to technological complexity and opaqueness, exceptionally difficult for the average consumer to understand whether what is presented to them is fair (for instance, from a choice perspective, price personalisation, etc. Lack of algorithmic transparency and the increased use of opaque algorithms determining product recommendations, prices, and content visibility lead to potential biases and unfair treatment that are all but impossible for the average consumer to discern. Lack of transparency can result in discriminatory practices, without the consumer in the digital environment being aware.

There have been **behavioural changes among consumers** over time. For instance, consumers are often omnichannel i.e. they use multiple channels when engaging in transactional decisions (e.g., online stores, physical stores and social media). They expect seamless integration between these different channels.

The above points have implications for the legal framework in that EU consumer law rules must **ensure fairness both offline and online** in recognition of this multi-channel environment. However, there may still be a need for **some differences in rules to tackle specific problems and challenges** (e.g. dark patterns in design interfaces, cancellation of online subscriptions). To ensure fairness, consumers in the digital environment may need additional protection for several reasons, such as to ensure protection from misleading information, such as fake reviews (already addressed through the MD), false and/ or non-transparent advertising), high levels of privacy and data security and to combat fraud and scams. Some of these areas fall within the remit of EU consumer law, whereas others such as data protection and privacy are covered through other EU laws. Other areas may represent a legal gap, with uncertainty as to how far consumer law could address these problems in future. A further key issue is how far consumers can be better protected by aligning different pieces of law by including provisions that reference existing requirements (e.g. GDPR, protection of sensitive data).

Information asymmetry-related problems experienced by consumers when making transactional decisions and purchases from traders have significantly evolved in the context of the rapid growth of the digital markets and services. Some legal academics and consumer associations have argued that digital asymmetries are markedly different in character.

Linked to the question of consumer vulnerability is the broader issue of information asymmetries in the digital environment. In this regard, BEUC has argued that consumers face three types of digital asymmetries¹⁴:

- **Structural and architectural asymmetry**: rooted in control of the choice architecture

¹⁴ CONSUMER PROTECTION 2.0: Structural asymmetries in digital consumer markets (2021), BEUC commissioned research by independent experts. EU March 2021, Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax and Joanna Strycharz

https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

of the service and access to data (and the related difficulty of verifying compliant use of data in the supply chain);

- **Relational dimension asymmetry:** as the bargaining power of the consumer is low – they may either accept or leave, with very limited alternatives;
- **Knowledge-based asymmetry,** as the trader benefits from detailed insights about the consumer while the consumer often knows (or understands) very little of how the trader and the service operate.

The BEUC report argues that *“in digital marketplaces, most if not all consumers are potentially vulnerable. Instead of singling out certain groups of consumers, digital vulnerability describes 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”*. The report also argues that *“Regulatory attention should shift from defining vulnerability or sorting out particular users under the concept of vulnerability towards tackling the sources of vulnerability, which comprise digital asymmetry”*. The above typology is important in framing the study overall, given the need to explore whether the EU consumer law framework is fit for purpose, given that digital asymmetries may differ from traditional information and knowledge asymmetries between traders and consumers in the offline environment.

However, the position may not be as clear-cut as the above typology implies. Whilst there are concerns regarding digital asymmetries being pronounced due to the persistence of problems such as dark patterns, equally, the digital environment provides consumers with greater opportunities to access information. For instance, there are tools to support consumers such as virtual assistants, price comparison websites and advisory and recommendation tools that serve as potentially neutral information intermediaries between consumers and traders (e.g. making price comparisons and other types of assessments of the characteristics and comparative merits and drawbacks of different products and services). Collectively, these tools may help to partially mitigate digital information asymmetries. It is also worth noting that informational asymmetries can also be common when consumers engage in offline transactions.

Further investigation of the issues of digital vulnerability and digital asymmetries among consumers are explored in the case study on consumer vulnerability (see Annex 5).

1.4.2.2 Average consumer

The notion of an average consumer was developed by the case law of the CJEU and then, subsequently, for the first time codified by the UCPD. The notion relies on an assumed level of knowledge of a typical consumer that is then used to help determine what constitutes an unfair practice. In Recital 18, the UCPD defines an average consumer as *“a consumer who is reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors, as interpreted by the European Court of Justice”*. A distinction is that whereas consumer vulnerability (see next sub-section) is defined in the Directive’s core text, the average consumer is defined in the recitals. As noted by Durovic (2014)¹⁵, the Commission’s rationale for putting this in the recitals was that *“the prescription of a definition would protect further evolution of the standard of the average consumer through the jurisprudence of the CJEU”*. The relevance of the concept of an average consumer is to make it clear that the unfairness test in the UCPD needs to be made against a common understanding that an average consumer has a reasonable degree of judgement in making decisions relating to purchases and transactions (online, offline). This is important as the concept of an average consumer differs from that of a vulnerable consumer, also defined in

¹⁵ The Impact of the Unfair Commercial Practices Directive (2005/29/EC) on Contract Law, Mateja Đurović (2014), European University Institute, Department of Law
https://cadmus.eui.eu/bitstream/handle/1814/34559/Durovic_2014.pdf?sequence=2&isAllowed=y

the UCPD, as discussed below.

1.4.2.3 Consumer vulnerability

Consumer vulnerability is an important consumer protection issue and firmly embedded within the EU consumer law acquis, as a definition of consumer vulnerability is provided in Art. 5(3) of the UCPD. The definition of vulnerability relates to the personal characteristics of the consumer, such as their age. Art. 5(3) UCPD states: *“Commercial practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group.”* According to a leading legal academic, this is an ambiguous term and there is a lack of clarity as to how this definition is meant to be interpreted in CJEU or national case law. As noted by Kaprou¹⁶¹⁷, *“consumer vulnerability signifies that consumers are not a homogenous group and some require a higher level of protection than others.”* Accordingly, in current policy discourse, there is a debate as to whether the current definition remains appropriate, or whether the concept of consumer vulnerability should be broadened. Individuals may have multiple characteristics of vulnerability, which raises questions as to how effective and relevant a category-based approach to defining vulnerability is.

The OECD report on Consumer Vulnerability in the Digital Age from June 2023 confirms the phenomenon of the evolving conceptualisation of consumer vulnerability in academic literature. BEUC has argued that consumer vulnerability is not only linked to personal vulnerabilities but in the digital age, consumers face a variety of digital asymmetries, some informational, others structural. Moreover, situational vulnerabilities may affect all consumers to a greater or lesser extent. Balanced against this argument, some EU trader representative associations have argued that whilst vulnerability is increasingly complex, the law must be implementable and that it would be difficult for them to consider multiple different types of vulnerabilities.

The Commission’s interpretation of vulnerability can be found in the UCPD Guidance, which states: *“The concept of vulnerability is not limited to the characteristics listed in Article 5(3), as it covers also context-dependent vulnerabilities. Multi-dimensional forms of vulnerability are particularly acute in the digital environment, which is increasingly characterised by data collection on socio-demographic characteristics but also personal or psychological characteristics, such as interests, preferences, psychological profile and mood.”* The Commission also stated that *“(…) the benchmark of an average or vulnerable consumer can be modulated to the target group and, if the practice is highly personalised, even formulated from the perspective of a single person who was subject to the specific personalisation. (...) The concept of vulnerability in the UCPD is dynamic and situational, meaning, for instance, that a consumer can be vulnerable in one situation but not in others. For example, certain consumers may be particularly susceptible to personalised persuasion practices in the digital environment, while less so in brick-and-mortar shops and other offline environments.”*

The issue of consumer vulnerability was assessed through a dedicated case study. However, issues around vulnerability are also considered in the case studies on aggressive practices, subscription renewals and personalised advertising. All case studies are provided in Annex 5. It can again be recalled that beyond specific groups of consumers who may have vulnerable characteristics, all consumers can be vulnerable in certain circumstances and at particular points in time (situational vulnerabilities when engaging in online transactions, for instance).

¹⁶ ‘The current legal definition of vulnerable consumers in the UCPD: benefits and limitations of a focus on personal attributes’, Eleni Kaprou - <https://bura.brunel.ac.uk/bitstream/2438/19635/5/FullText.pdf>

¹⁷ See Chapter 4, The legal definition of ‘vulnerable’ consumers in the UCPD: benefits and limitations of a focus on personal attributes, Eleni Kaprou, *Vulnerable Consumers and the Law*: <https://www.routledge.com/Vulnerable-Consumers-and-the-Law-Consumer-Protection-and-Access-to-Justice/Riefa-Saintier/p/book/9780367555184>

1.4.3 Intervention logic

The Better Regulation Guidelines require evaluations and fitness check assessments to be based on an intervention logic. The logic mapping specifies how the EU consumer law framework is expected to work and the assumed underlying logic based on the causal chain linkages that should lead to the intended changes. These in turn should bring about the achievement of the legislation's general and specific objectives e.g. a high level of consumer protection and the fostering of the (digital) single market. The way in which the implementation of activities and inputs relevant to the application of EU consumer law is expected to lead to digital fairness through causal pathways at the output-results level and the results-to-impacts levels is also considered.

In summary, the intervention logic explains the relationship between the:

- Needs, problems, and challenges that EU consumer law is meant to address;
- The objectives (differentiated between 'general' of a more strategic nature, and 'specific' operational goals);
- The inputs and activities required to achieve these objectives. Inputs include human resources required to develop, monitor, and update EU consumer law and supporting guidance and financial resources for these activities and regarding enforcement; and
- The outputs, results, and impacts (corresponding to the short, medium and longer-term outcomes).

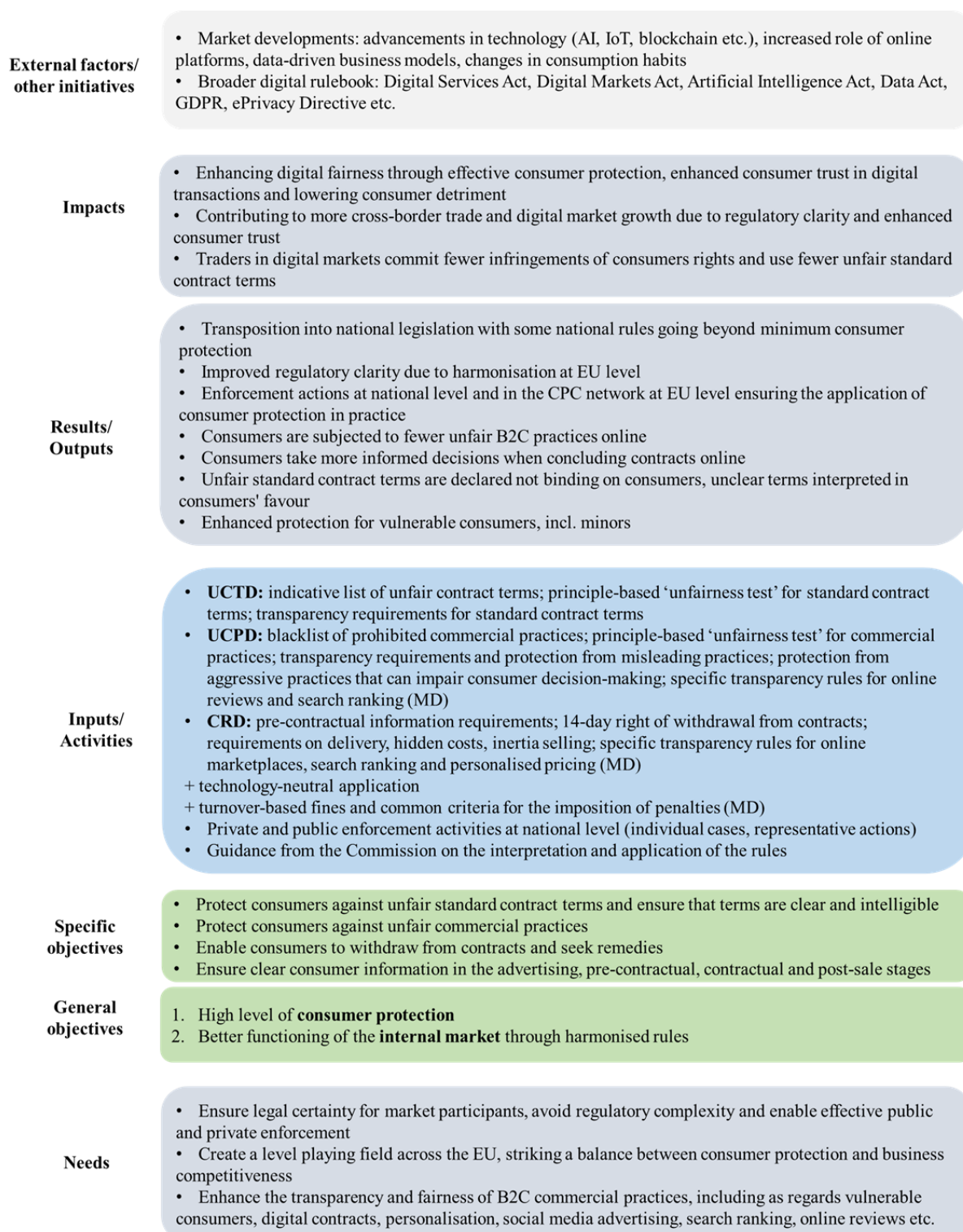
The logic mapping also considers:

- The **role of external factors in influencing outcomes at results and impacts levels**. Such factors include: technological developments, developments in digital markets and services, changes in business practices over time, the evolving EU and global regulatory context, for instance, whether more specific rules have been introduced in some MS and / or in some third countries.
- **“Cause and effect” relationships relating to the theory of change (ToC) and the extent of contribution** being made by EU consumer law to achieving its core objectives, but also in contributing to digital fairness. The ToC was tested by the consultancy team through an examination of causal chains at the output-results level and results-impact pathways, to check how far working assumptions regarding the anticipated outcomes of EU consumer law in terms of benefits and impacts stand up to the evidence base developed from an assessment of desk research and stakeholder consultation feedback on the perceived benefits.

This assessment was based on desk research using a combination of sources, i.e. the legal texts of the three Directives respectively, including the recitals and key articles, guidance documents and previous impact assessment studies where available (e.g. for the Consumer Rights Directive and Modernisation Directive).

The intervention logic sets out the links between the expected impacts (mirroring the general objectives) and the expected results (mirroring the specific objectives) which are designed to address the problems being tackled through EU consumer legislation and the inputs, activities and processes leading to the outcomes, namely the various rules, information obligations and transparency requirements for traders, and inputs such as the development of national lists of unfair contract terms (UCTD) and of an EU-wide list of unfair commercial practices (UCPD).

Figure 1.1 – Intervention logic – EU consumer law and fostering of digital fairness



Source: DG JUST

As the EU consumer law framework currently stands, the concept of digital fairness is not an explicit regulatory objective in the three pieces of law within scope. However, in the context of the existing objective of achieving high levels of consumer protection within a single market context, given the rapid development of digital markets and services in the European economy, it is arguably an implicit objective in that the application and effective enforcement of EU consumer law (including where relevant its interaction with other legislation e.g. EU laws to ensure data protection and privacy, recent digital laws) should lead to more digital fairness. The working assumption in this study was therefore that digital fairness is a desired outcome that should increasingly materialise at the impacts level, given the body of EU consumer law that already exists, the development of new and recent legislation applied in parallel with consumer law, and given the growth in the digital single market across different sectors, such as the platform economy, subscription economy etc. Achieving digital fairness in practice however supposes that certain pre-conditions are met, namely that:

1. There are high levels of compliance by traders across a diverse range of digital services and markets (e.g. ranging from e-commerce players through to online platforms and marketplaces and social media influencers).
2. EU consumer law is effectively transposed by Member States, with national regulatory divergence avoided to prevent barriers to trade within the single market;
3. EU consumer law is applied across the EU in a sufficiently harmonised manner;
4. EU consumer law is well-known by all traders (across the EU and outside of the EU) that target EU consumers and enforced effectively by Consumer Protection Authorities and through private enforcement;
5. The legislation works as intended, with EU consumer law being designed to be applied in a technology-neutral manner both online and offline.

Regarding **needs**, the body of EU consumer legislation needs to be fit for purpose to address both online and offline transactions in parallel, given the growing importance of Europe's digital economy. As the legislation has been designed in a technology-neutral way, the three Directives can be applied in the digital environment, but equally to offline transactions. A further need was to check whether the scope of EU consumer protection law is sufficient to address new practices, trends and developments in digital markets and services. An additional need is to enhance the transparency and fairness of B2C practices in the digital environment to increase legal certainty for consumers and traders. Lastly, there is a need to ensure the smooth operation of markets for digital content and services in the Single Market, by striking the right balance between a high level of consumer protection and business competitiveness.

Additional information regarding **problems and challenges** that the legislation aims to address is provided in the case studies presented in Annex 5, which consider practices identified as potentially problematic. However, given this is an evaluation rather than an impact assessment, the analysis is presented only at a high level as the study's purpose is to identify the extent to which problems have already been addressed through existing legislation, or if there remains regulatory uncertainty and/ or legal gaps. In a possible future impact assessment, problems would be analysed in further detail as part of logic mapping, in the form of a problem definition and problem tree.

The intervention logic sets out the **inter-linkages between the three Directives**, the UCPD, UCTD and CRD, along with the changes from the MD to strengthen the treatment of certain digital aspects of the legal regime and the enforcement of EU consumer law through the harmonisation of redress possibilities in the case of unfair commercial practices and the harmonisation of penalties for consumer law breaches through the establishment of turnover-based fines (for infringements subject to coordinated actions under the Consumer Protection Cooperation (CPC) Regulation) and common indicative and non-exhaustive criteria, with broad alignment in the scale of those fines with other EU legislation, notably the GDPR and

competition law.

The latter is relevant to achieving digital fairness given that many traders in the digital environment operate cross-border and/ or on a pan-European basis. The previous situation prior to the MD was that ‘effective, proportionate and dissuasive’ penalties for infringements were required under the UCPD and CRD, however, these varied significantly between MS. In the case of the UCTD, requirements were not set out explicitly, but according to feedback received during the study via the ECC-NET, 11 MS included penalties in national laws that national authorities could use to sanction non-compliant enterprises, suggesting regulatory divergence in the application and scale of penalties.

Turning to the **general objectives**, there are strong commonalities across the UCPD, CRD and UCTD Directives. These aim to foster high levels of consumer trust and empowerment and to bring about a better functioning of the internal market through harmonised rules. **Specific objectives** are Directive-specific. Both the general and specific objectives are explained in the following table:

Table 1-3 – General and specific objectives of EU consumer law in scope

Directive	General objectives	Specific objectives
UCPD	<ul style="list-style-type: none"> • Achieve a high level of consumer protection across the EU. • Effective functioning of the internal market. 	<ul style="list-style-type: none"> • Protect consumers against unfair (including aggressive and misleading) B2C commercial practices by prohibiting a broad range of unfair business practices. • Ensure better consumer information in advertising, contractual and post-sale stages.
UCTD	<ul style="list-style-type: none"> • Achieve a high level of consumer protection across the EU. • Effective functioning of the internal market. 	<ul style="list-style-type: none"> • Protect consumers against unfair standard contract terms through approximation of national laws. • Ensure that standard contract terms are expressed in a clear and intelligible manner.
CRD	<ul style="list-style-type: none"> • Achieve a high level of consumer protection across the EU. • Effective functioning of the internal market. 	<ul style="list-style-type: none"> • Align and harmonise national consumer rules for distance selling and doorstep selling contracts. • Better consumer pre-contractual information. • Effective 14-day right of withdrawal. • Protect consumers against delivery problems, hidden costs, inertia selling.
Modernisation Directive	<ul style="list-style-type: none"> • Strengthen consumer protection by modernising existing EU consumer legislation and enhancing enforcement measures and harmonising penalties. 	<ul style="list-style-type: none"> • Harmonisation of consumer rights in respect of physical and digital goods and services. • Introduces strengthened rights to redress and stronger penalties for breaches of EU consumer law.

Source: DG JUST, authors’ own research

The inputs and activities include the technology-neutral application of the Directives, an important feature of the regulatory design of EU consumer law. This approach is designed to facilitate the development of digital markets, and to avoid stifling innovation and competitiveness, whilst still ensuring high levels of consumer protection. Further examples of inputs include the development of supporting Commission guidance, with examples of which types of practice are prohibited. A further element of the Directives' implementation is public and private enforcement activities. The crucial role of national CPAs should be stressed in undertaking enforcement activities against non-compliant traders, including in the digital sphere. As considered under an evaluation question (EQ) specifically relating to the effectiveness of enforcement (see EQ5 the effectiveness criterion), there appear to be limited numbers of legal cases in the digital area, suggesting enforcement remains a challenge, but the increased complexity of digital cases should also be recognised meaning potentially fewer cases, but these sometimes having a strategic deterrent effect.

Enforcement activities at the output level include legal proceedings, leading to the emergence of national case law and CJEU rulings in testing and clarifying the application of EU consumer law. In addition, some Member States, such as Germany, rely on private law as a means of ensuring effective enforcement of EU consumer law.

A further **input** is the recent updating of two guidance documents on the interpretation and application of the rules, the Guidance on the UCPD and the Guidance on the CRD which were previously updated in 2021. In addition, the Commission has developed new guidance on the UCTD and the PID published in 2019 and 2021 respectively.¹⁸ Whilst non-legally binding, the interpretative guidance nonetheless plays an important role in supporting the Directives' application, with an especially important role in promoting digital fairness. For example, the UCPD Guidance includes a specific section on interpreting the Directive's application in the digital environment (Section 4.2 – Digital Sector), referring to issues such as online platforms and their commercial practices, the transparency of search results, data-driven practices and dark patterns and influencer marketing. As the legislation adopts a technology-neutral, general principles-based approach, the interpretative guidance contains more detailed examples of the scope of the law and its application in the digital environment, including examples of case law. In contrast, the CRD is more technical legislation, which does not reflect the general principle-based approach. It focuses particularly on e-commerce in the context of distance selling contracts.

Regarding inputs and activities at the Directive level, these vary by Directive. Selected examples provide an illustration:

- The UCPD includes a blacklist of prohibited practices that are always considered to be automatically unfair, three general clauses which aim to protect consumers and a principle-based general 'unfairness test' relating to the trader's 'professional diligence'. Since the MD came into application, further changes to the UCPD were made through regulatory amendments including the introduction of specific transparency rules for ads and the trustworthiness of online consumer reviews, as well as new requirements on the transparency of ranking of search results for online platforms.
- The CRD includes pre-contractual information requirements, a 14-day harmonised right of withdrawal (RoW), and rules on delivery, hidden costs and inertia selling. More recent inputs to strengthen digital fairness are specific transparency rules for online marketplaces and personalised pricing.
- The UCTD – includes an indicative and non-exhaustive list of contract terms which may be regarded as unfair, which some Member States implemented as a 'black list'

¹⁸ Guidance on the interpretation and application of Article 6a of Directive 98/6/EC of the European Parliament and of the Council on consumer protection in the indication of the prices of products offered to consumers.

or a 'grey list'¹⁹ of unfair terms, while the Directive only sets minimum standards. Most importantly, the UCTD imposes a principle-based 'unfairness test' for contract terms in consumer contracts as well as fulfilment of transparency requirements in relation to these terms.

The way in which the **Directives' objectives and inputs and activities are transformed into outputs, results and impacts** is now considered. Regarding **outputs**, the Directives are transposed into national legislation and notified to the Commission. Some national rules may go beyond the minimum requirements in EU consumer protection legislation. Whilst two of the three Directives are maximum harmonisation Directives, there are still a few regulatory choices available to Member States, meaning that there is some divergence in national application (the extent to which this is the case explored later in the report under the evaluation criterion "coherence").

Furthermore, Member States may adopt measures that fall outside of the scope of these Directives, e.g. introduce additional limitations to B2C commercial practices for objectives other than the protection of the economic interests of consumers. However, as considered in an EQ under effectiveness concerning the emergence of national legislation in areas such as influencer marketing and the avoidance of subscription traps through a cancellation button, there is an issue around whether national rules risk undermining the effectiveness of the harmonisation character of EU consumer law, especially for the UCPD as most of the new national rules relate to unfair and / or aggressive practices covered by this Directive.

Further examples of outputs are the results of private and public enforcement cases taking place at national level. Public enforcement is led by national CPAs, who play a role in market monitoring to check compliance with the requirements in the three Directives, but also in leading enforcement actions against traders if evidence of non-compliance is identified. Private enforcement takes the form of legal cases by consumers and their representative organisations against traders through the court systems, leading to the emergence of national case law and CJEU rulings. Selected examples of case law have been incorporated into some of the case studies and have been used in addressing some EQs, such as testing which factors constitute unfair, misleading or aggressive practices in influencing transactional decisions. This is included because of its importance in clarifying the interpretation of the legislation, and in highlighting the role of enforcement as a factor influencing the effectiveness of the Directives' implementation.

Turning to **results (intermediate outcomes)**, there are some common elements across EU consumer law whereas others vary by Directive. Regarding results common across the pieces of law within scope, effective transposition, application and enforcement of the Directives ought to lead to higher compliance levels with EU consumer law by traders in the digital environment, thereby eliminating unnecessary costs for compliant traders. However, in practice, it is very difficult to obtain accurate data on compliance levels across different areas of the digital economy and across all digital markets and services. Through the sweeps, some evidence emerged of widespread non-compliance in certain areas, such as not complying with the requirement to clearly communicate the 14 day Right of Withdrawal (RoW), which was the case in 46% of websites examined. However, this issue is nuanced by the fact that some traders prefer to offer a 30-day cancellation period or even indefinite cancellation rights in the case of digital services.

A further result common across the three Directives – stemming from enforcement activities at the input level and legal cases at the output level - is that regulatory clarity should improve due to national case law and CJEU rulings in response to any new and emerging business practices. National case law appears to be more prevalent under the UCTD and UCPD than with the CRD. For instance, there have been legal cases to clarify the circumstances in which

¹⁹ The grey list includes contract terms that are presumed to be unfair (the trader can rebut this presumption), whereas the black list contains a list of prohibited contract terms.

consumers may have been misled into making a transactional decision they would not otherwise have made.

Regarding **Directive-specific results**, under the UCTD, unfair contract terms must be declared as non-binding on consumers and unclear terms must be interpreted in consumers' favour. Under the UCPD, the introduction of greater information requirements to strengthen transparency means that consumers should be taking better informed decisions due to having improved pre-contractual, contractual, and post-contractual information available, and they are subjected to fewer unfair B2C practices online. Regarding the CRD, results are that consumers can take more informed decisions due to more relevant information being provided to them during the pre-contractual and contractual stages, and thus, are better protected when they conclude contracts online. The MD also strengthened information provision to consumers when purchasing goods or services through online marketplaces (e.g. requirement to inform consumers whether a seller is a private individual or a professional trader).

Regarding **impacts (longer-term outcomes)**, positive outcomes should stem from the application of the three Directives which are mutually reinforcing (covering different aspects of the transaction process) as benefits should accrue from (1) preventing unfair, misleading and aggressive commercial practices, (2) prohibiting unfair contract terms and (3) ensuring the adequate provision to consumers of pre-contractual, contractual and (where appropriate) post-contractual information to reduce the chances of consumers being misled.

Implementing consumer law effectively should contribute to achieving the desired outcomes identified. The types of benefits that should in theory be manifested are: (1) High levels of consumer protection, ultimately, bringing about 'digital fairness', (2) Enhanced consumer trust (3) Reduced barriers to cross-border trade through a maximum harmonisation approach, (4) Reduced barriers to cross-border trade through a maximum harmonisation approach, at least for the UCPD and the CRD, (5) Reduced non-compliance levels with EU consumer law requirements among traders in digital markets and (6) A reduction in levels of consumer detriment. There are also Directive-specific examples of impacts, such as fewer unfair / unclear standard contract terms (UCTD), with fewer unfair B2C commercial practices (UCPD) and improvements in the efficacy of consumer contract law, given the symbiotic relationship between the UCPD and the UCTD.²⁰

The crucial role of **external factors** has also been considered as these have an influence on the way in which the intervention logic (and associated causal chains) works in practice compared with how the logic is expected to work in theory. Among these factors are developments in digital markets and services, such as advances in technology (growing use of AI, the IoT and connected products, the use of smart contracts etc.), the increased role of online platforms and their transition into marketplaces, data-driven business models and changes in monetisation models, etc. In addition, in particular sub-sectors, there are also rapid developments. For instance, the influencer phenomenon has grown and livestreaming by influencers has become a new trend and business model, raising new questions regarding how to strengthen enforcement of hidden advertising rules under the UCPD. These developments raise issues around how existing EU legislation is applied to new and emerging developments and trends in digital markets impacting consumers and the protection of their existing legal rights. It also raises issues around the extent to which there are legal gaps emerging due to new business practices.

Further external factors include significant developments in the EU policy and regulatory framework through the revision of existing EU laws, the entry into application of new legislation, and the development of additional new legislative proposals in the past 5 years. These have had an impact on EU consumer law. Some legal developments have raised issues regarding the need to strengthen coherence between EU consumer law and other pieces of

²⁰ The Impact of the Unfair Commercial Practices Directive (2005/29/EC) on Contract Law, Mateja Đurović
https://cadmus.eui.eu/bitstream/handle/1814/34559/Durovic_2014.pdf?sequence=2&isAllowed=y

law applicable to digital markets and services. This raises an issue whether in certain areas more specific rules may be needed to reflect technological and market developments and to reflect the complex interplay between consumer law, digital and data laws, as witnessed in emerging case law, albeit with a relatively small number of cases so far.

The **increasing complexity of the regulatory landscape** has led to a situation where legal cases and complaints from consumers and consumer associations sometimes relate to the interplay between several different pieces of legislation. For example, the BEUC complaint²¹ against TikTok concerned the infringement of several EU legal instruments regarding the same subject matter and related also to B2C commercial practices (UCPD, CRD, UCTD, GDPR, AVMSD). A consideration for the fitness check is that **much of the relevant EU legal corpus is either new** (e.g. the DSA, DMA) **or is at the regulatory proposal or negotiation stage**. Therefore, the implications for EU consumer law of changes to the EU legal framework in the case of new digital market and services and data protection and privacy-related legislation are already adopted and evident but in other instances, they are still under consideration. A provisional assessment in this regard is provided under the 'external coherence' section under key evaluation issues.

The contribution of EU consumer law to meeting its general and specific objectives needs to differentiate between (1) what has been achieved directly through the application of the UCTD, UCPD and the CRD, supported by regulatory amendments made through the MD, and (2) how far developments in digital markets and services have impacted on the nature and extent of the contribution of these Directives to ensuring digital fairness for consumers.

²¹ <https://www.beuc.eu/tiktok>

2 Problematic practices in the digital environment

2.1 Problematic practices

This section sets out the current situation on problematic practices. It outlines practices identified as being potentially problematic based on previous literature and stakeholder feedback, including in many recent studies for the European Commission's DG JUST and identified through a series of CPC network-organised sweeps. This section explains the concept and considers the prevalence of problematic practices. Individual problematic practices are then considered (drawing on survey data, interview feedback and case study findings). Whereas stakeholder feedback is considered for some problematic practices within the research questions, feedback is brief and summary for other questions as there are supporting case studies in annex which consider the issues raised and stakeholder feedback in further detail.

Possible solutions to some of these challenges are mentioned, but considered more thoroughly under the 'relevance' criterion.

2.1.1 Overview of problematic practices in a fitness check context

Commercial practices and contract terms with the potential to be characterised as unfair or otherwise problematic are heterogeneous. A distinction can be made conceptually between:

- 1) Problematic commercial practices 'covered by' the material scope of EU consumer law or wider EU legislation.** For instance, certain dark patterns could be covered by the UCPD's general clauses, with some specific examples covered in Annex prohibitions. The dark patterns topic is also addressed in the Commission's UCPD guidance document. However, under the general principles-based approach, such practices are subject to a case-by-case assessment by a national court or CPA. Dark patterns have also been explicitly prohibited for platforms under the DSA, although limited in scope only to platforms (not individual traders) and excluding B2C dark patterns that are 'covered by' the UCPD. However, even if there are existing provisions that could be applied to problematic practices, consideration should still be given as to how to improve the way in which they are dealt with in the existing legal framework (e.g. strengthening the legal framework through more explicit provisions in future, mentioning in the recitals, or keeping the legislation unchanged but instead updating the Guidance with further examples of unacceptable practices).
- 2) Non-compliance by traders with existing EU consumer laws and/or insufficient enforcement.** This may relate to where commercial practices or contract terms have already been directly or indirectly regulated, but where problematic practices persist in the European market. It could however also relate to **insufficient regulatory certainty**, as some CPAs, Ministries and consumer associations perceived there to be a need for more specific rules concerning some practices e.g. dark patterns, online subscriptions, the use of sensitive data for personalised advertising.

Even where problematic practices are deemed to be 'covered' by the material scope of the EU legislation, **the application of the laws leaves room for interpretation**. Some practices may technically fall within EU consumer law's scope under the general clauses (e.g. the general unfairness test in the UCPD covers dark patterns), but a case-by-case assessment is still required to determine whether a particular commercial practice is allowed or prohibited by traders and subsequently by enforcement authorities. Whilst the previous fitness check in 2017 and this study found that the majority of stakeholders perceive the general principles based approach to have been effective, there may be grey areas in terms of the delineation of what constitutes an

acceptable or a non-acceptable commercial practice as the legislation remains at a general principles level (although there are some practices that are expressly prohibited through Annex 1 of the UCPD and the blacklisting approach, and in national blacklists of unfair terms).

- 3) Problematic practices not (yet) addressed in EU legislation.** There are examples of other commercial practices where there are consumer protection concerns, but the regulatory framework does not explicitly address these practices. This may be the case, for instance, for practices driven by new and emerging features in digital markets, or where new technologies pose new challenges for the protection of consumers, and the legal framework is still catching up. It may also be the case for practices where discretion has been left to national law, e.g. concerning the cancellation of contracts. Here, the challenge for this study is to review these practices and to arrive at findings as to whether specific practices may warrant future regulatory intervention, or need to be addressed through soft law measures (e.g. guidance documents, codes of conducts among traders to avoid certain practices or to foster good practice).

EQ1 – What are the main problematic digital business-to-consumer (“B2C”) practices identified in digital trade from a consumer protection perspective? How prevalent are these practices, and has there been an increase in the past few years?

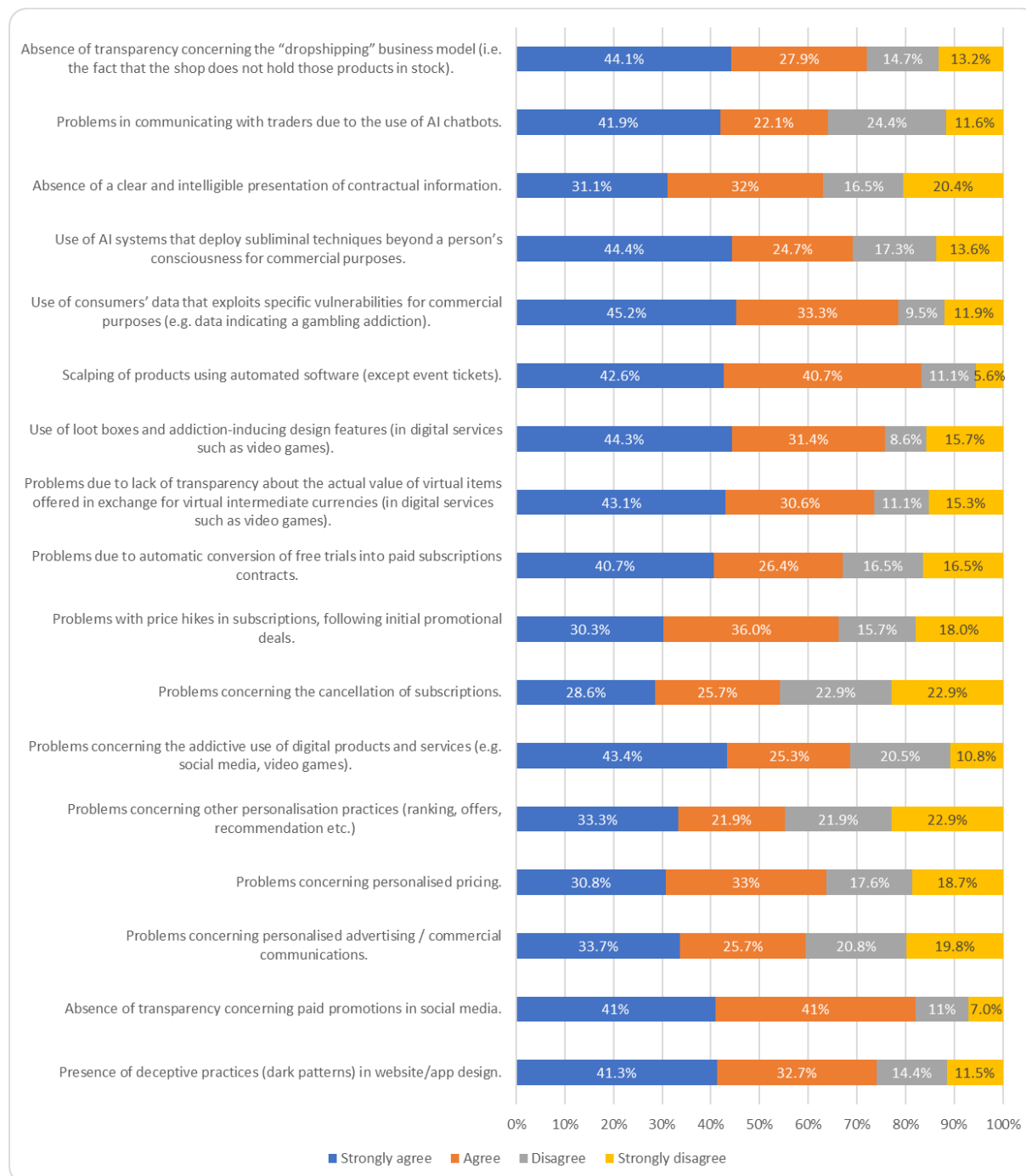
This EQ firstly considers what are the problematic digital business-to-consumer (“B2C”) practices identified in digital trade from a consumer protection perspective. It considers the prevalence of these practices and how far there has been an increase in problematic digital practices that may challenge the ongoing effectiveness (and relevance) of the Directives. The assessment draws on a combination of interview feedback, position papers, desk research. Reference should also be made to the detailed case studies in Annex 5, which address a series of problematic B2C practices, such as personalisation practices, aggressive practices, deceptive designs in websites and apps, social commerce, etc.

This section introduces many of the problematic practices in the digital environment under review through this fitness check study. The Fitness Check has investigated practices identified as raising consumer protection concerns, such as dark patterns, problems with digital subscriptions, personalisation practices, influencer marketing, digital addiction etc.

Collectively, the above commercial practices have been identified as raising questions as to whether elements within these practices should be further regulated and/ or more explicitly regulated or simply better enforced. These different aspects have been termed **‘problematic practices.’**

Overall, as shown in the graph below, the majority of respondents (taking the strongly agree and agree responses combined) in the targeted stakeholder agree that **all** the listed practices are perceived to be problematic. Therefore, such findings support the need to concentrate attention on the problematic practices mentioned in the question below. Among the main trends are that 43.4% of respondents strongly agreed (and a further 25.3% agreed) that the problems concerning the addictive use of digital products and services is a problematic practice.

Figure 2.1 - To what extent do you agree or disagree that the following practices are problematic? (no. = 105)



Source: targeted survey

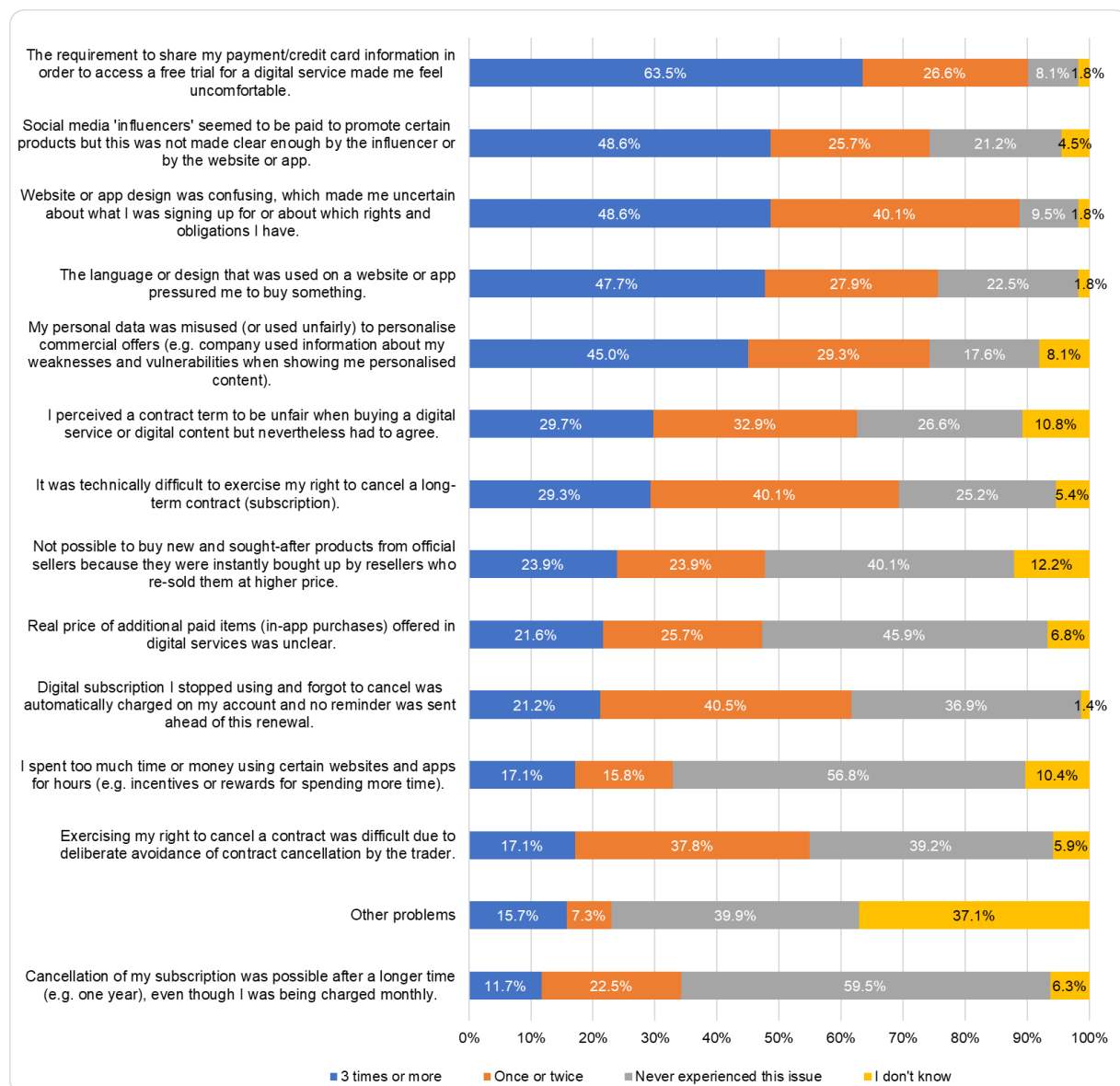
Additional primary survey data was gathered through the public consultation survey and consumer survey of 10,000 consumers. Moreover, some data from the BEUC survey of 5,000 consumers (2023) to support their position paper on digital fairness is also highlighted.²²

The consumer responses to the public consultation indicated an overarching message that consumers encounter challenges in asserting their rights in the digital environment, in certain

²² BEUC, Connected, but unfairly treated: Consumer survey results on the fairness of the online environment https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf

areas relatively frequently in the course of a year, even if some of these have already been legislated for:

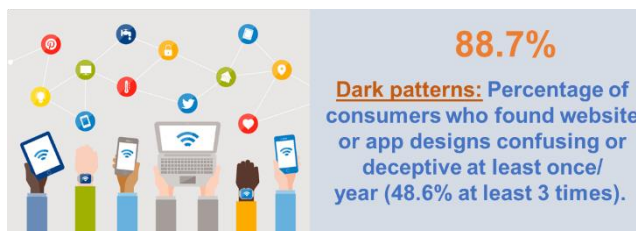
Figure 2.2 - In the past 12 months, have you experienced any of the following problems online, and if yes, what frequency? (n=222)



Source: public consultation survey

- The most frequently occurring problematic practice mentioned was the **requirement to share payment/credit card information to access a free trial** for a digital service, which is not illegal under existing consumer laws. 91% of consumers faced this issue, with 63.5% (141 out of 222) experiencing it three times a year or more.

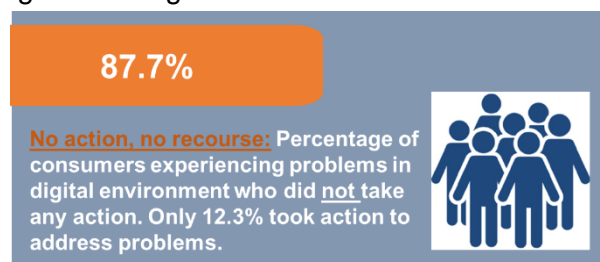
- 74.3% experienced a **lack of adequate disclosure regarding paid promotions** by social media influencers.
- 88.7% mentioned they found website or app designs confusing or deceptive (48.6% 3 times or more and 40.1% once or twice with only 9.5% never experiencing this issue), suggesting that **dark patterns** remain a problem.
- Digital subscriptions were also viewed as being **difficult to cancel** (69.4%) and consumers were automatically charged for a subscription **without receiving any reminder about the renewal** (61.7%).
- Less frequently mentioned were challenges in cancelling contracts due to the **long period required before cancellations** (34.2%) and issues around **digital addiction** to websites and apps (32.9%).



Regarding the **geographic location of traders** with whom consumers encountered problems, approximately one-third were located in the consumer's own Member State, one-third in another EU Member State and one-third were traders from third countries. To exercise their rights, consumers need to have knowledge that such rights exist and can be applied in the digital environment. They also need to know how to resolve complaints and disputes.

Regarding **knowledge of EU consumer rights in the digital environment**, 21.6% (48 out of 222 consumers) stated that they had sufficient knowledge, 55.4% felt they had had some knowledge, and 23% felt they did not have enough knowledge.

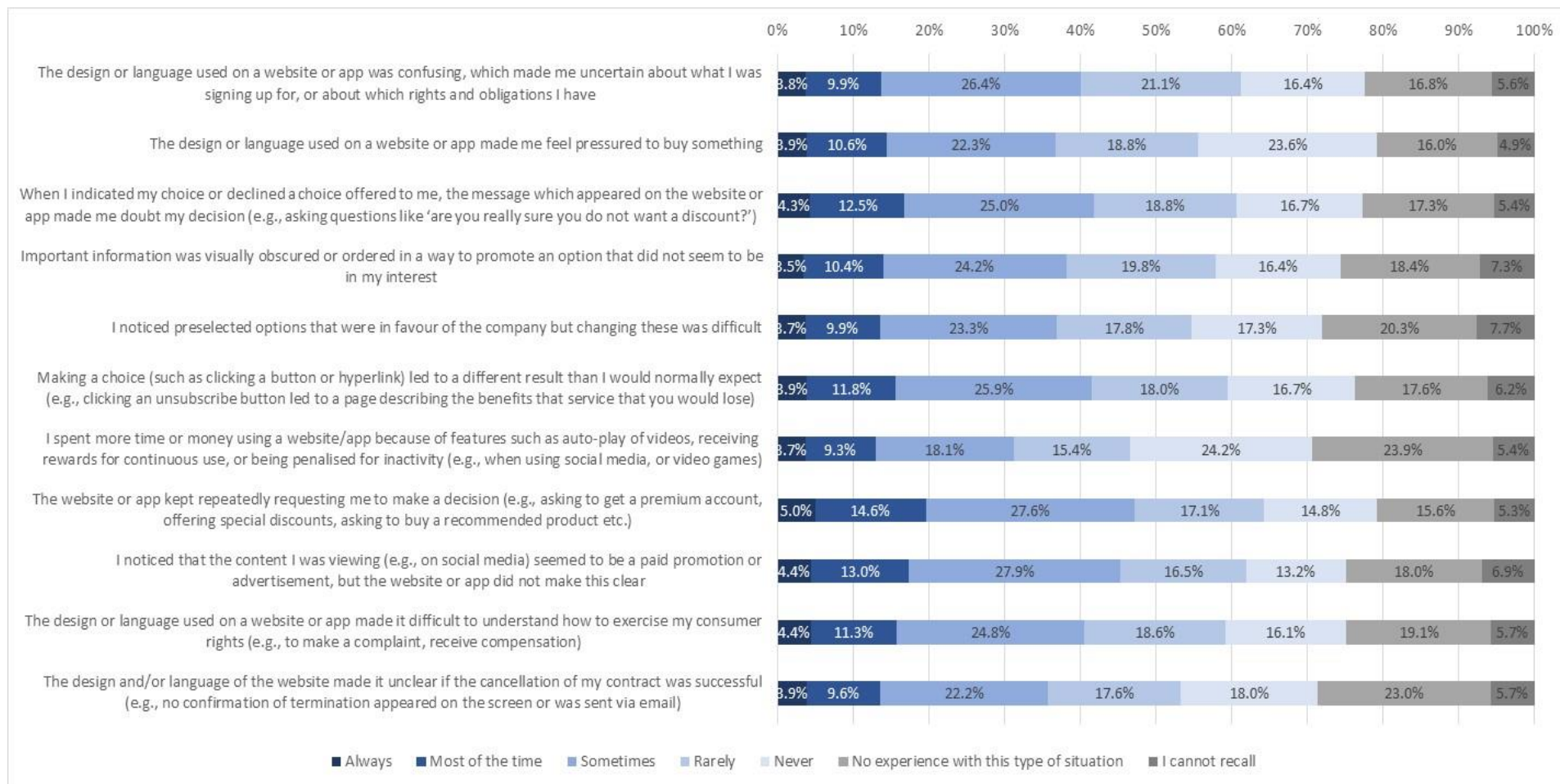
However, only **12.3% of consumers took action** to address these problems and **87.7% did not take any action to solve problems** they encountered. This suggests that consumers were not generally confident that a positive outcome could be achieved, the relatively small amount of detriment involved in individual cases meaning it may have not been worth their time pursuing a complaint, etc.



However, only 32 consumers answered this question and most (59.4% or 19 out of 32 respondents) complained to the service provider, such as a website or app developer. Some complained to consumer protection authorities (25%), and a further 6% to a consumer association. Reflecting the cross-border dimension of complaints, a further 3% (1) complained to a European Consumer Centre (ECC) belonging to the ECC Network. The role of Alternative Dispute Resolution (ADR) mechanisms should also be highlighted, although only 3.1% (1) mentioned they had brought the dispute to the attention of an ADR, such as a Consumer Ombudsman.

To complement the public consultation, a representative **consumer survey** (10,000 consumers) was undertaken. The questions included perceptions of problematic practices, which broadly reflect the problems raised in the public consultation as well as additional issues, such as **more granular findings on specific dark patterns** used, as shown in the following graph.

Figure 2.3 - In the past 12 months, have you experienced the following situations online? (n=10000)



Source: Fitness Check - consumer survey based on national panels in 10 EU countries, conducted in June and July, 2023

In addition, the **BEUC survey of 5,000 consumers**²³ undertaken as a contribution to their fitness check position paper found that:

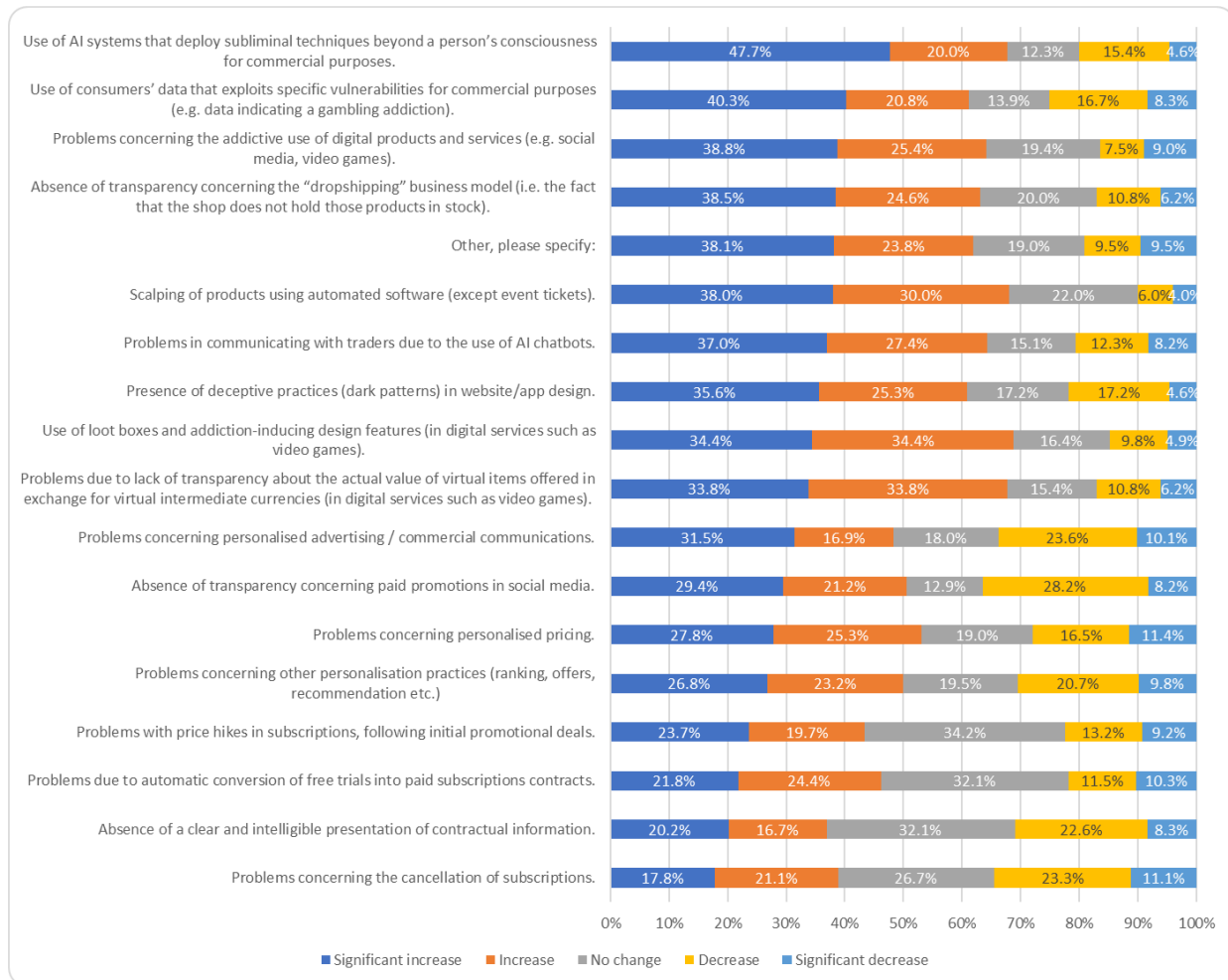
- Despite spending more and more time online, **fewer than half of consumers (43%) feel in control of the content they are shown and the decisions they take.**
- **Respondents disapprove of being monitored and tracked online.** Less than one in five consider it fair that they are targeted with ads based on their lives or vulnerabilities.
- Consumers would like **greater regulation of influencers on social media.** Almost half (44%) of people who come across influencers saw them promoting possible scams or problematic products.
- **Children's protection online.** 75% of consumers agree that children need more protection from online tracking and from being influenced by digital services.

Some further findings are relevant to consumer protection. These relate to the need to further strengthen enforcement, and the importance of allowing consumers greater control of how their data is used.

To complement the public consultation and consumer survey, in the targeted survey, stakeholders were asked about the extent to which there had been an increase or decrease in the frequency of different problematic B2C digital practices. The results are shown below:

²³ BEUC's full survey findings which required involvement of national consumer associations are available from: <[BEUC-X-2023-020 Consultation paper REFIT consumer law digital fairness.pdf](#)>

Figure 2.4 - In the past five years, how far have the following potentially problematic B2C digital practices increased or decreased in frequency? (N = 90)



Source: targeted survey

The problematic practice which was perceived to have increased the most in frequency was the use of loot boxes and addiction-inducing design features, as 68.8% respondents noted either an increase or a significant increase (combined). Some of the other response options also received perceptions that problematic practices had increased or significantly increased, such as: scalping practices using automated software beyond tickets sales (the latter already regulated in the MD) (68.0%), the use of AI systems that deploy subliminal techniques beyond a person's consciousness for commercial purposes (67.7%), problems concerning the lack of transparency regarding the value of virtual items in virtual currencies (67.6%), problems concerning the use of AI chat bots when communicating with traders (64.4%), deceptive practices on websites (60.9%), problems with personalised pricing (53.1%) and other personalisation practices (50.0%), including personalised advertising (48.4%), lack of transparency concerning paid promotions (50.6%), the automatic conversion of free trials into paid subscriptions without sufficient precontractual information and/ or warning reminders (46.2%). The findings corroborate those from the other surveys, which also found that consumers experienced problems frequently, despite some practices already being prohibited.

Whereas some problematic practices are already legislated, other business practices are not

prohibited (e.g. provision of payment/credit card information to access a free trial), but may be perceived as problematic or unwelcome by consumers. It should be recalled when interpreting this data that not all stakeholders agree that each practice mentioned is problematic. For instance, whereas all stakeholders agree that pressure selling should be illegal, and that inflated prices due to sought-after products being bought up and resold is problematic, for an issue such as being asked for payment information upfront, whereas consumers and their representative associations view this practice as problematic and deterring them from signing up, many trader associations viewed this as being a legitimate business practice.

In the public consultation, most respondents considered that EU consumer law positively impacts on the following areas relevant for consumer well-being (very or rather positive impact): **protecting consumers against unfair commercial practices** (71.4%), **protection of vulnerable consumers** (53.4%), **ensuring adequate information to consumers** (53.8%). Regarding the **impact on cross-border e-commerce**, **42% considered it to be positive** (9.0% stated very positive and 33.0% rather positive), which was higher than the corresponding percentages for the **increase in national e-commerce** (5.4% very positive and 28.5% rather positive).

However, only 27.2% of respondents thought that the **impact on prices** had been positive (5% very positive, 22.2% quite positive) whereas 30% considered the impact to be neutral. Regarding the highest totals for negative impacts, the most frequently mentioned response option was **the competitiveness of EU businesses compared with non-EU businesses** (15.8% negative and 10.4% very negative). The Figure below from the targeted survey highlights the extent to which the three Directives have been effective in tackling problematic practices. The main finding was the three Directives are perceived to have been at least somewhat effective in tackling a variety of problematic practices. The **top five problematic practices** where EU consumer law was seen by respondents as having been **most effective** (i.e. combining the very and quite effective responses only) in tackling these issues was as follows:

1. Absence of a clear and intelligible presentation of contractual information (70.8% total either very or quite effective, 25.3% 'very effective' and 45.5% 'quite effective');
2. Absence of transparency concerning paid promotions in social media (67.7% total, with 27.1% very effective and 40.6% quite effective);
3. Problems concerning personalised advertising / commercial communications (65.0% total, with 28.0% stating very effective and 37.0% quite effective);
4. Presence of deceptive practices in dark design (61.5% in total, with 24.0% very effective and 37.5% quite effective);
5. Problems due to the lack of transparency about the actual value of virtual items and currencies (total of 53.1% consisting of 20.3% very effective and 32.8% quite effective).

The bottom five areas regarding where EU consumer law was perceived as having been **least effective** in addressing problematic practices (combining the not very effective and not effective at all responses) were:

1. Use of AI systems that deploy subliminal techniques beyond a person's consciousness for commercial purposes. A total of **63.7%** said either not very effective, or not effective at all (namely 30.4% not very effective and 33.3% not effective at all).
2. Problems concerning the addictive use of digital products and services (e.g. social media, video games). A total of **61.7%** said either not very effective or not effective at all (namely 38.4% not very effective and 23.3% not effective at all).
3. Use of consumers' data that exploits specific vulnerabilities for commercial purposes

(e.g. data indicating a gambling addiction). A total of **59.8%** said either not very effective or not effective at all (i.e. 33.8% not very effective and 26.0% not effective at all).

4. Use of loot boxes and addiction-inducing design features (in digital services such as video games). A total of **59.1%** said either not very effective or not effective at all (namely 28.8% not very effective and 30.3% not effective at all).
5. Problems due to automatic conversion of free trials into paid subscriptions contracts. A total of **58.4%** said either not very effective or not effective at all, i.e. 32.6% not very effective and 25.8% not effective at all).

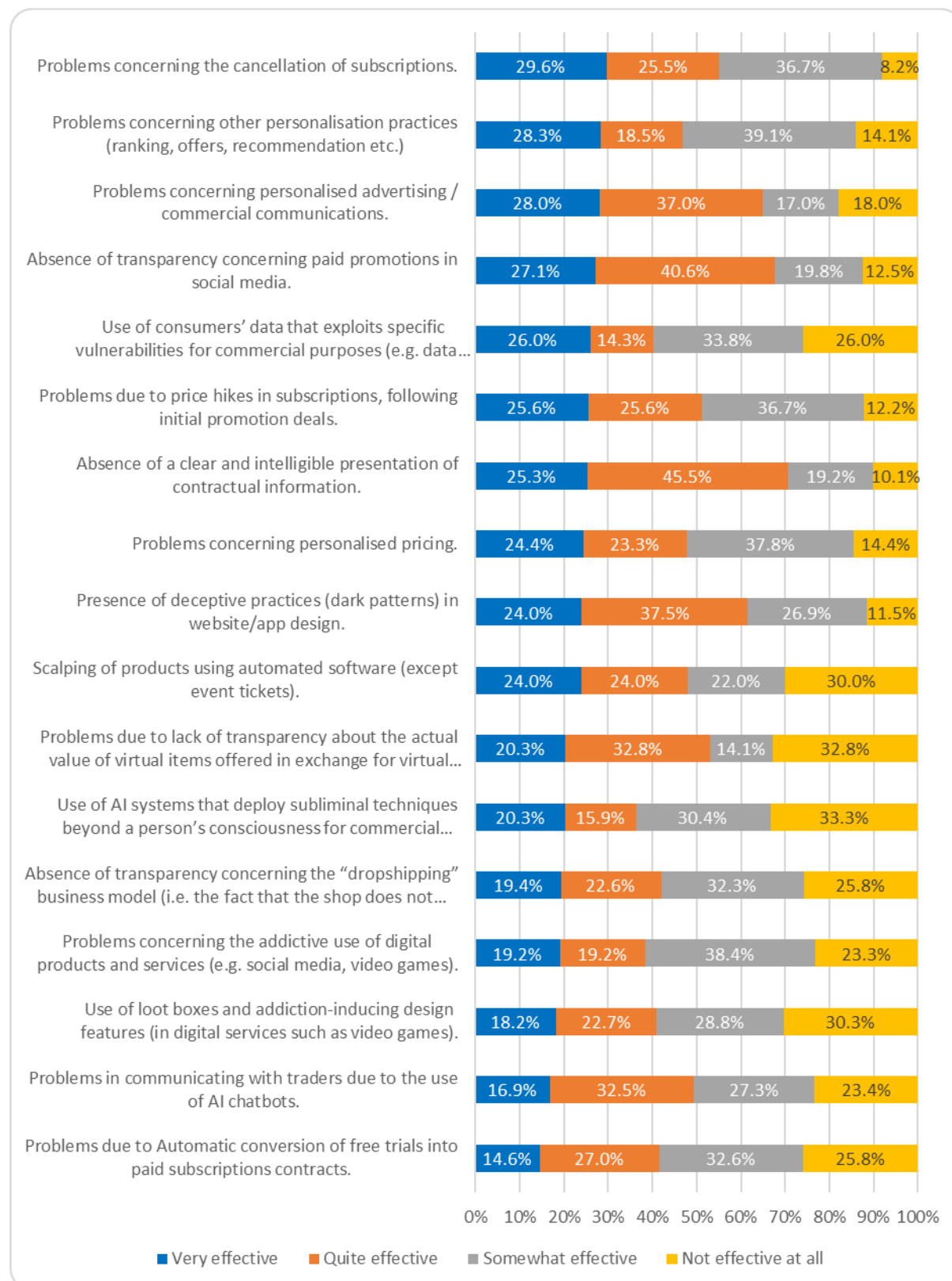
Some of the findings above regarding whether EU consumer law is presently effective are perhaps unsurprising given that some of these problematic practices are not presently addressed directly in EU consumer law.

Regarding the scalping of products using automated software, 52% of respondents in total said either that existing EU consumer laws are not very effective or not effective at all (namely 30% not very effective and 22% not effective at all). The MD specifically aimed to tackle the use of bots to inflate prices of event tickets but a lot of the problem with scalper bots appears to be more general.

It is interesting that clear differences in the survey results by type of problematic practice have emerged. For instance, whereas the three Directives were collectively seen as having been reasonably effective in addressing unfair or misleading practices in the use of data for personalised advertising, considerably fewer respondents perceived that the legal framework had been effective in addressing personalised pricing, but these topics are not explicitly regulated through EU consumer law, other than the disclosure requirement recently introduced on personalised pricing (whereas personalised advertising is regulated for platforms in the DSA, but not directly in terms of any specific rules in the UCPD).

Nonetheless, these problematic practices were still identified as such overall based on responses to other questions.

Figure 2.5 - To what extent have the three core EU consumer law Directives been effective in tackling perceived problematic digital B2C practices? (n=104).



Source: targeted survey

2.1.2 Dark patterns

RQ1 – What problems do consumers face with dark patterns? How far are dark patterns sufficiently addressed by the UCPD and in other pieces of EU law?

Dark patterns are ways of designing user interfaces in a way that tricks or misleads users into doing things they might not have done otherwise. Whilst such manipulative practices are used by some traders to increase sales or to foster engagement, they may cause harm to users' autonomy, trust, and well-being. They are deceptive and take advantage of people's biases, emotions, and mental limitations.

The **public consultation survey** showed that a combined 88.7% of consumers found website or app designs confusing or deceptive at least once per year (48.6% experienced this problem 3 times or more annually, 40.1% once or twice in the same period). Only 9.5% never experience this issue.

Table 2-1 - In the past 12 months, have you experienced any of the following problems online? The design of a website or app was confusing, which made me uncertain about what I was signing up for or about which rights and obligations I have.

Response options	Number	%
3 times or more	108	48.6%
Once or twice	89	40.1%
Never experienced this issue	21	9.5%
I don't know	4	1.8%
Grand Total	222	100.0%

Source: public consultation

The consumer survey 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%).

Furthermore, the **targeted survey** highlighted the point that over the last five years, dark patterns have increased. 35.6% of the respondents detected a significant increase, whilst only 17.2% observed a significant decrease in the frequency of such problematic practice taking place. Various studies and sweeps by CPAs have confirmed that consumers continue to experience different types of dark patterns. Specific examples of dark patterns include “confirm-shaming”, often mentioned by BEUC in position papers, but also forced registrations, problematic pre-selections/ manipulations of design interfaces presenting choices, toying with emotions, and the inclusion of trick questions, among others. However, the only dark patterns that are 100% prohibited are fake countdown timers and low stock messages which are mentioned in the Annex of the UCPD, which outlines prohibitive practices. This means that traders must interpret the law and how to comply with it using only the UCPD guidance. CPAs also have the difficult task of trying to interpret the legislation given that specific practices are not prohibited explicitly and are therefore arguably open to interpretation. Some specific examples based on literature review are now shown, followed by stakeholder feedback from the interviews and public and targeted consultation position papers.

The 2022 **behavioural study on dark patterns** for the European Commission²⁴ found that consumers continue to face a series of problems in respect of dark patterns, i.e. manipulative interface and choice architecture designs. The study included mystery shopping, digital ethnography, literature review, expert interviews, workshops, and two behavioural experiments. It found that unfair practices are incredibly prevalent (97% of the most popular websites and apps used by EU consumers contained at least one dark pattern) and rarely used in isolation. Rather, it is instead common to combine several dark patterns in one interface design. The study noted that the trend is predicted to continue, *“with businesses making increased use of personalisation practices and combining these with dark patterns”*. The most common dark patterns were 1) hidden information/false hierarchy, 2) preselection, 3) nagging, 4) difficult cancellations, and 5) forced registration. There were no significant differences in terms of prevalence across websites and mobile apps, Member States or EU/non-EU traders, nor between different types of websites. However, the most used type of dark patterns differed per sector, e.g. ‘fake timers’ more prevalent in ecommerce and online marketplaces, while ‘nagging’ more prevalent in health/fitness.

The study also confirmed that there is a lack of consumer awareness regarding the use of unfair practices, but once an unfair practice is identified, consumers perceive these practices negatively. The average consumer’s ability to discern the use of these practices is rather

²⁴ Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>

limited and, raising even more concern, consumers appear to accept the presence of unfair practices as part of their normal digital experience and have become accustomed to them. Dark patterns and manipulative personalisation can lead to financial harm, loss of autonomy and privacy, cognitive burdens, mental harm, as well as raise concerns in terms of collective welfare due to detrimental effects on competition, price transparency and trust in the market.

The behavioural experiments proved that dark patterns had a statistically significant impact on the transactional decision of both average and vulnerable consumers. Vulnerable consumers were slightly more affected than average consumers, especially older participants and those with lower educational attainment levels. The average probability of making inconsistent choices when exposed to dark patterns was 50.89% for vulnerable consumers (5.42% increase compared to the control group) and 47.24% for average consumers (9.44% increase compared to the control group). Furthermore, transparency-based remedies were found to be ineffective for both average and vulnerable consumers. The study suggested that more effective regulatory options (as seen in the control group) would be the prohibition of specific practices and the imposition of a fair/neutral design obligation.

Moreover, research published by the **Consumer Protection Cooperation (CPC) network** on dark patterns in January 2023²⁵ found that there remained problems with dark patterns on retail websites. An assessment by the CPAs involved in the sweep to assess manipulative online practices found that out of 148 of 399 online shops screened:

- **42 websites used fake countdown timers** with deadlines to purchase specific products (putting pressures on consumers to make purchasing decisions they would not otherwise have made);
- **54 websites directed consumers** towards certain choices - from subscriptions to more expensive products or delivery options - either through their visual design or choice of language;
- **70 websites were found to be hiding important information or making it less visible for consumers.** For example, this included information related to delivery costs, the composition/content of products, or on the availability of a cheaper option. 23 websites were hiding information with the aim of manipulating consumers into entering into subscriptions;
- The sweep also included the **apps of 102 of the websites screened**, 27 of which also deployed at least one of the three categories of dark patterns.

Furthermore, in 2023, the **Dutch Consumer and Market Authority (ACM)** conducted a sweep (using automated methods) of websites to check for **fake countdown timers** (a prohibited practice UCPD Annex point no 7).²⁶ In their investigation, ACM found that the use of fake countdown timers continues to be a problem, although the problem appears to be less pronounced than before this practice was added to the blacklist. Hundreds of countdown timers were identified, for example: “3 hours remain to take advantage of this deal”. Whilst the use of timers is not prohibited, the timers must have actual consequences: if the deal is genuinely available for a limited amount of time, it must disappear once the timer reaches zero, otherwise it is an unfair and misleading practice. In 41 cases, the ACM discovered that deals were still available after the timer had reached zero, or that a new timer started with the same or even a better offer, practices that are prohibited. An earlier study by the same CPA found that there was evidence of dark patterns operating at scale²⁷. The relatively low number

²⁵ See press release on the findings from the consumer sweep January 2023 on manipulative practices. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418

²⁶ [ACM confronts online stores using misleading countdown timers with their practices | ACM.nl](https://www.acm.nl/en/news/2023-01-26-acm-confronts-online-stores-using-misleading-countdown-timers-with-their-practices)

²⁷ Mathur, A. et al. (2019) ‘Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites’, *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), p. 81:1-81:32. Available at: <https://doi.org/10.1145/3359183>.

of fake countdown timers is an indication that traders may be less likely to avoid using dark patterns if that specific practice is clearly prohibited in the UCPD blacklist.

The **2023 OECD report on dark patterns**²⁸ found that there are increasing concerns that dark commercial patterns (commonly found in online user interfaces and steer, deceive, coerce, or manipulate consumers into making choices that often are not in their best interests) may cause ‘**substantial consumer detriment**’. The report proposes a working definition of dark commercial patterns, sets out evidence of their prevalence, effectiveness and harms, and identifies possible policy and enforcement responses to assist consumer policy makers and authorities in addressing them. The OECD study also highlights some interesting findings regarding how far different types of technologies and devices may impact the extent to which dark patterns trick consumers into making purchases (transactional decisions they would not otherwise have made), which is outlawed in the UCPD. “*Evidence points to the greater effectiveness of dark patterns on mobile devices or smaller screens, where information is less prominent (Utz et al., 2019[78]; Strahilevitz, 2021). Supporting such findings, other research shows greater cognitive effort is required to distinguish news from covert advertising on mobile screens (Amazeen, 2021)*”.

Among the main findings regarding the impacts of dark patterns on consumers in the OECD study were that there are considerable harms of dark patterns to consumers, for instance, the impacts on consumer autonomy and personal and structural consumer detriment. The OECD report also notes that dark patterns literature has highlighted personal detriment as the primary normative concern about dark patterns (Mathur, Kshirsagar and Mayer, 2021). The personal consumer detriment from dark patterns can be broadly divided into three broad categories: i) financial loss, ii) privacy harms, and iii) psychological detriment and time loss. These harms are likely to be cumulative where multiple dark patterns are employed at once and are often interrelated (e.g. financial and privacy loss can also lead to psychological detriment).

A **2022 BEUC position paper**²⁹ addresses the concerns surrounding choice architecture in the digital economy, particularly on online platforms. BEUC notes how the **digital economy has brought benefits to consumers** but BEUC recognises that there is **a growing need to examine how choices are designed and presented**, particularly in online platforms. BEUC presents an illustrative typology of dark patterns to give a sense of their classification and the issues facing consumers, while acknowledging that these are not always clearly applicable, and practices are sure to evolve as businesses innovate their use of data and algorithmic design, however the list is as follows, practices that:

- (1) *Make certain decisions more prominent or easier to make;*
- (2) *Create a false feeling of urgency/scarcity and a ‘fear of missing out’ (e.g., the use of a “high-demand” message);*
- (3) *Shame consumers (i.e., creating a feeling of guilt via social influence or peer pressure (e.g., “confirm-shaming”));*
- (4) *Obstruct or confusing consumers (e.g., use of questions with “double negative”);*
- (5) *Blind consumers (e.g., sneaking items into the basket).*

Digitalisation enables businesses to experiment with user-centred design, user experience design, and testing methods to influence consumer behaviour based on personal data. These **dark patterns are widespread and can manipulate transactions and obtain consent for further manipulation**. Instances of unfair business practices and misleading advertisements have been identified in cases involving companies like Booking.com, Facebook, X (formerly Twitter), Google, and Amazon. Consumer law cases targeting these dark patterns have been

²⁸ Dark commercial patterns, OECD Digital Economy papers

<https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm>, October 2022 No. 336

²⁹ BEUC position paper, “Dark patterns” and the EU consumer law acquis: Recommendations for better enforcement and reform (2022)

on the rise, highlighting the need for better enforcement and protection. The report emphasises the increasing use of techniques to influence consumer decisions across markets. To address this issue, the report provides recommendations for both improved enforcement and reform, **focusing on a horizontal consumer law perspective**.

Focusing on the UCPD, but also drawing from the CRD, BEUC made several recommendations to address the issue of dark patterns and consumer protection in relation to the existing legal framework relating to this study, which are structured by Directive. For example, regarding the UCPD, BEUC suggested an updated concept of transactional decisions, and new rules on the burden of proof to reflect digital asymmetry and the continuing prevalence of dark patterns, despite them already being covered in theory in the UCPD's general provisions. Regarding the CRD, the suggestion was to implement a specific obligation to include a contract cancellation button to make cancelling as easy as entering into a contract (something already done in the most recent 2021 UCPD guidance) to prevent consumers being locked into subscriptions.

In order to assess whether there are legal gaps in addressing dark patterns, it is first necessary to describe the legal framework.

The **UCPD regulates dark patterns through the general principles-based clauses in the Directive (i.e. Articles 5-9) and Annex I blacklist**. For instance, if a particular website or platform has incorporated deceptive design, then such practices would be considered as unfair, misleading or aggressive. Traders and CPAs must undertake a case-by-case assessment to determine if a given business practice relating to website or platform design is a dark practice or acceptable. Only a few dark patterns are explicitly prohibited (e.g. fake urgency in Annex I point 7). Given the absence of more explicit and specific rules regarding dark patterns, the UCPD guidance explains how to interpret the general principles-based clauses applicable in the case of (potential suspected) dark patterns.

However, it should be recalled that the wider EU legal framework has evolved significantly in terms of how dark patterns are addressed beyond the UCPD, with new rules being introduced through the DSA (applicable from January 1st, 2024), and rules included in the GDPR (applicable from 25th May 2018). This necessitates consideration by the Commission as to whether the lack of specific rules or a definition in the UCPD continues to achieve the desired regulatory and enforcement objectives.

Dark patterns related to personal data may also constitute a breach of GDPR, regarding the principles outlined in Article 5, namely:

- The requirements for consent to be given freely, specific and informed (Article 4 (11)). Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
- Article 7 GDPR (conditions for consent), which outlines transparency requirements around consent; and
- The principle of privacy by design (Article 25 GDPR).

The GDPR complements other EU legislation by making it clear that consumers should opt-in transparently in terms of providing their personal data. However, dark patterns could be used to trick users into handing over personal data whose ultimate purpose may be unclear. Data protection authorities (DPAs) are responsible for sanctioning the use of deceptive design patterns if these breach GDPR requirements. The EDPB³⁰ developed examples of dark patterns on platforms in Guidelines of March 2022 which provided best practice

³⁰ European Data Protection Board (EDPB)'s Guidelines on "Dark patterns in social media platform interfaces" of 14.03.2022.

recommendations to designers and social media platform providers on how to assess and avoid dark / deceptive patterns in social media interfaces that violate the GDPR's requirements. The guidelines were updated in March 2023³¹.

Whilst until recently there was no definition of a dark pattern in EU law, in the past few years, this has begun to change. EU legislation has been evolving and although "attention-capture dark patterns" are not explicitly covered, in the DSA, a legal definition of dark patterns has emerged in Article 25(1) DSA, even if only applicable to platforms. It 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 service to make free and informed decisions*". According to Recital 67 of the DSA: "*Dark patterns*" are practices that aim to **prevent users from making autonomous and informed choices or decisions**. This is less about the content of (e.g. advertising) statements, but primarily about the "structure, design or functionalities" of online interfaces (i.e. primarily websites or apps), for example because the choices are not presented in a neutral way, in that certain choices are given more prominences through "visual, auditory or other components". In addition, **Article 31 (1) DSA on Compliance by design** provides that online platforms allowing consumers to conclude distance contracts with traders shall ensure that its online interface is designed and organised in a way that enables traders to comply with their obligations regarding pre-contractual information, compliance and product safety information under applicable Union law.

Stakeholders interviewed mentioned that despite progress made in defining dark patterns through the DSA, it remains difficult to provide a precise definition. Trader associations and traders pointed out that over time, the concept has been broadened, with some studies defining dark patterns in a very broad sense, making rules prohibiting such practices in the UCPD more difficult to be applied. It is important to note that the prohibition only covers online platforms (not the non-intermediary websites or apps of individual traders, such as retailers or video games), and Article 25(2) excludes from the scope of the prohibition practices that fall under the UCPD or GDPR. This effectively carves B2C dark patterns out of the scope of the prohibition. Many stakeholders as well as a legal academic interviewed during the study commented that it is unclear which are the circumstances in which a platform should follow the more specific UCPD rules on dark patterns or those set out in the DSA. Overall, this interplay was the most common coherence issue reported in the Fitness Check.

Whereas the UCPD prohibits dark patterns under the general provisions, Art. 25 of the DSA (Online interface design and organisation) prohibits dark patterns explicitly:

"Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions".

Some stakeholders such as consumer associations perceived the DSA's explicit prohibition of dark patterns to be a clearer means of regulating the persistent problem of dark patterns than the UCPD, where it is presently regulated through the general principles clauses but not explicitly mentioned, apart from in the interpretative guidance. However, other stakeholders, especially trader associations and individual traders disagreed strongly, as in their view, it has been clear since the UCPD was adopted that dark patterns are prohibited, and rather, the problem lies with weak enforcement and higher than acceptable levels of non-compliance, even if the levels of non-compliance were not possible to quantify by trader associations or traders interviewed, nor by CPAs.

³¹ EDBP Guidelines 2.0 - Deceptive design patterns in social media platform interfaces: how to recognise and avoid them - https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

Whether this constitutes a legal 'gap' therefore depends on the differing views of stakeholders by type. Consumer associations and some Ministries and CPAs would prefer a more detailed legal framework that explicitly prohibits dark patterns, whereas others are content with the status quo, and viewed the legislation as already being sufficiently clear. A legal academic from ELI interviewed mentioned the potential importance of standards in ensuring that dark patterns are tackled effectively, for instance, the possibility of having a set of standards governing website design, e.g. clarifying the means of exercising the RoW and of cancelling a contract.

The role of voluntary codes of conduct by industry was also highlighted as a mechanism for eliminating dark patterns. For instance, in its public consultation position paper response, Apple stated that in their guidance in the App Store *"apps must respect the user's permission settings and not attempt to manipulate, trick, or force people to consent to unnecessary data access (App Review Guidelines 5.1 (iv))"*.

A national Ministry in France responding to the public consultation pointed out that as the UCPD and the DSA are meant to be mutually exclusive, the Commission needs to make clearer the distinction between when the DSA should be applied and when the UCPD should be applied in respect of dark patterns. It is *"important to understand if there are specific types of Dark Patterns which do not fall under the category of unfair commercial practices"*. This issue could perhaps be addressed through updating of the guidance documents to support the legislation's application.

Dark patterns were also addressed during legislative discussions around the **Digital Markets Act (DMA)**. Both the European Parliament and the Council decided in their respective positions to address dark patterns in the context of the anti-circumvention clause included in Article 13 of the DMA. It is important to highlight that this is not a general prohibition of the use of dark patterns but only in connection with the compliance assessment of the DMA obligations. In this regard, the UCPD is fully applicable to any dark pattern deployed by traders who would be designated as 'gatekeepers' under the DMA. Article 13 (4) DMA on anti-circumvention measures states that *"the gatekeeper shall not engage in any behaviour that undermines effective compliance with the obligations of Articles 5, 6 and 7 regardless of whether that behaviour is of a contractual, commercial or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design"*. This provision is further complemented by explanations in Recital 70 of the DMA which forbids dark patterns' use only by gatekeepers and only within the context of attempts to circumvent other obligations already put in place by the DMA: *"Gatekeepers should not engage in behaviour that would undermine the effectiveness of the prohibitions and obligations laid down in this Regulation. Such behaviour includes the design used by the gatekeeper, the presentation of end-user choices in a non-neutral manner, or using the structure, function or manner of operation of a user interface or a part thereof to subvert or impair user autonomy, decision-making, or choice"*.

Stakeholder feedback on dark patterns and impacts

Stakeholders taking part in this study had varying opinions on the role of dark patterns, reflective of their perspectives as distinctly consumer or trader-focused entities or individuals.

Beyond the public consultation and targeted survey results mentioned earlier, qualitative feedback on dark patterns was also received through the interview programme and in position papers. Academic opinion on the issue of dark patterns tends to favour a consumer protection focused view of necessary actions, and has a degree of cynicism towards the views of industry representatives. For example, the **European Law Institute** strongly agreed in their position paper that there is a particular need for strong protection against digital dark patterns.

BEUC recommended that a **horizontal prohibition on dark patterns** reinforced by an anti-circumvention clause (such a clause was recently included in the DMA) is needed in the

UCPD. It also advocated the development of a list of prohibitions of the most commonly-used dark patterns in Annex I to the Directive. In an earlier separate position paper specifically focusing on dark patterns³², BEUC suggested creating a database of unfair design practices. The paper also suggested that CPAs involved in the CPC Network should enforce the UCPD against dark patterns more consistently. BEUC also suggested providing guidance to enterprises on the legal boundaries of persuasion to avoid designing choice architecture in a way that can be unfair and misleading.

The **Finnish Consumer and Competition Authority** highlighted the prevalence of dark patterns across devices and platforms, emphasising the complexity of design practices. They argue for the consolidation of legislation related to dark patterns to prevent a fragmented legal landscape.

It is important to note that the harms caused by dark patterns may not be apparent to consumers or even to businesses employing them. In their response, the **Consumer Council Taenk Denmark** proposes shifting the burden of proof regarding the use of dark patterns/manipulative designs as it would be difficult for consumers and CPAs to understand the underlying web architecture. However, they would not wish to see increased regulatory burden placed on traders. **UFC-Que Choisir** expressed support for prohibiting dark patterns in website design and suggested introducing a general prohibition on misleading interfaces.

Independent Retail Europe believes that the issue remains stronger enforcement against dark patterns across the Single Market, and better education of consumers, insisting that the legal framework is inherently sufficient in its protection of consumers.

Svensk Handel (Swedish Trade Federation) noted firstly that it is important to define what a “dark pattern” is. They observed that the Commission had performed a sweep which found “manipulative online practices”. However, they do not agree that a practice where a website is presented in a way that directs the customer towards a purchase should be considered as a “dark pattern”. For example, in a physical store, the products are presented in a way to entice customers into make purchasing decisions, which is legitimate provided it is not done unfairly or manipulatively. Many interviewees from the trader association representative side in different sectors similarly called for a definition of dark patterns and clarifications as to which specific dark patterns are outlawed, such as to provide regulatory certainty to traders.

The issue of **coherence between EU legislation concerning dark patterns** was also raised by multiple stakeholders. Several stakeholders pointed out that on the one hand, improvements have been made in regulating dark patterns through the DSA (which provides a detailed definition), and on the other, regulatory uncertainty because of the lack of (perceived) coherence of the legal framework. The DSA explicitly regulates dark patterns in web interface design, but the UCPD and GDPR rules on dark patterns are arguably less clear and explicit. A legal academic interviewed commented that it is unclear in which circumstances a platform should follow the more specific UCPD rules on dark patterns, as opposed to those set out in the DSA, even if the latter was set up under the principle of *lex specialis*. This was also referred to in BEUC’s position paper for the fitness check³³, which also noted that there is legal uncertainty regarding dark patterns. Whilst the DSA contains a prohibition on dark patterns in Article 25(1), in BEUC’s view:

“This provision is weakened by the exclusion of practices ‘covered by’ (sic) Directive 2005/29/EC (UCPD) or Regulation (EU) 2016/679 (General Data Protection Regulation) under Article 25(2). The wording used in Article 25(2) is unclear and likely to cause interpretative doubts, e.g. whether formal decisions must be issued first under

³² “DARK PATTERNS” AND THE EU CONSUMER LAW ACQUIS

https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patterns_paper.pdf

³³ TOWARDS EUROPEAN DIGITAL FAIRNESS - BEUC framing response paper for the REFIT consultation - https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf

the GDPR and the UCPD before the provision may apply. This may render the provision unusable in practice for situations affecting consumers".

The **national authority in France** responsible for consumer law also commented in their public consultation response that there is a need for further clarity as to when the DSA should be applied, as it was not clear if there are specific types of dark patterns which do not fall under the category of unfair commercial practices.

Conclusions – ongoing problems with dark patterns

The research has identified ongoing problems with dark patterns, as evidenced in consumer sweeps on manipulative practices by CPAs undertaken through the Consumer Protection Cooperation (CPC) network, and in the major study on dark patterns for the European Commission in 2022. These findings are further supported by other investigation findings, such as to the 2023 ACM action against fake timers. However, there are concerns among traders, and to some extent other stakeholders that it will not be possible to address dark patterns without a clear definition for legal purposes.

Whilst there was common agreement that several types of dark patterns can already be covered through the general principles-based clauses of the UCPD, there are concerns about poor enforcement and a lack of guidance for CPAs and traders as to how the prohibition of dark patterns should be enforced. Many stakeholders favour clarity and greater regulatory certainty on this issue.

Possible solutions to address the identified problems are provided under the relevance question on problematic practices and means of addressing them are provided under EQ14.

2.1.3 Aggressive practices

Aggressive practices were examined through a dedicated case study which considered those practices within or beyond dark patterns considered to be aggressive. Findings extracted from the case study are provided below. However, the detailed stakeholder feedback is provided in the case study itself.

RQ2(1): Which commercial practices qualify as “aggressive” in the digital environment?

As per Articles 8 and 9, 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** and causes them or is likely to cause them to make a transactional decision that they would not have made otherwise. This provision focuses on the alteration of the process to shape consumers’ will using **techniques that compromise their freedom of decision**³⁴. In addition, one must consider all the features and circumstances of such practice in its factual context. So, for a commercial practice to be aggressive, two conditions must be fulfilled: first, the practice must amount to harassment, coercion, or undue influence; second, the practice must be capable of significantly impairing the average consumer’s freedom of choice regarding the product.

Articles 8 and 9 refer to three forms of aggressive commercial practices: harassment, coercion, and undue influence. Yet, while Article 2 defines the latter, there is **no definition of harassment and coercion**. It is, therefore, necessary to discuss these:

- The Cambridge Dictionary³⁵ defines ‘**harassment**’ as behaviour that annoys or upsets someone.

³⁴ Pablo Fernández Carballo-Calero, Aggressive Commercial Practices in the Case Law of EU Member States, Journal of European Consumer and Market Law, Volume 5, Issue 6 (2016) pp.255-261.

³⁵ Cambridge University Press & Assessment, Cambridge Dictionary, 2023, available at: <https://dictionary.cambridge.org/>.

- The Cambridge Dictionary³⁶ defines '**coercion**' as using force to persuade someone to do something they are unwilling to do. UCPD Articles 8 and 9 also state that coercion includes using force, which is irrelevant to the digital environment (or just irrelevant, one could argue³⁷). The American Psychology Association³⁸ specifies that coercion is attempting to influence another person using threats, punishment, force, direct pressure, and other harmful forms of power.
- The UCPD indicates that '**undue influence**' means 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 decision³⁹. It is, therefore, clearer how the latter can apply to the digital environment based on the relational power asymmetry between traders and consumers. Based on this definition, for example, social media **influencers**' behaviour can, in some cases, amount to an aggressive commercial practice based on the use of '**undue influence**' linked to their relationship with their audience, often based on trust and a personal connection, which puts them in a position of power that they can exploit.

Yet, there might be overlaps between the three types of aggressive practices. It could be argued that influencers' practices can also amount to '**harassment**'. For example, there may be circumstances in which, during live-streaming shopping events, influencers aggressively promote products, using practices that pressure consumers into making purchases, if they pester them with follow-up communications or ask them to buy at a specific time (see case study on social commerce and social media influencers for a detailed assessment of such practices).

In addition, looking further than the definition of coercion mentioned above, **psychological coercion**, according to US Legal, includes theories of mind control or brainwashing. The risk of psychological coercion is relevant when the primary target audience of an influencer includes **vulnerable consumers**, such as children and young people. The latter is also one of the primary target audiences of the **gaming** industry, in which certain commercial practices can indeed be aggressive. These include selling practices related to loot boxes, in the case of which a significant impairment of choice or conduct might arise through **undue influence or coercion**. In their article on **virtual coercion** and the vulnerable consumer, P. Cartwright and R. Hyde suggest that offering loot boxes might fall under either of these concepts. They conclude that the absence of a definition of coercion introduces unnecessary uncertainties⁴⁰.

Other potentially aggressive practices include personalised advertising, notably as traders consider specific information about gamers' **vulnerabilities**, including using algorithms to target **addiction-prone players**. Where the trader collects data about a consumer and makes offers based on conclusions its algorithm draws about the individual, there is a strong argument that the trader is in a position of power, forming the basis for **undue influence**, which concretise if the trader exploits this position in a way that 'significantly limits the consumer's ability to make an informed decision'⁴¹.

More generally, the use of **online behavioural advertising** can lower the visibility of 'non-personalised' options, including adverts that do not exploit consumers' irrationalities based on

³⁶ Cambridge University Press & Assessment, Cambridge Dictionary, 2023, available at: <https://dictionary.cambridge.org/>.

³⁷ See Cartwright P. and Hyde R., Virtual coercion and the vulnerable consumer: 'loot boxes' as aggressive commercial practices, Legal Studies 42, pp. 555-575, University of Nottingham, Nottingham, UK, 15.01.2022, available at: <https://doi.org/10.1017/lst.2022.7>.

³⁸ American Psychology Association, APA Dictionary of Psychology, 2023, available at: <https://dictionary.apa.org/coercion>.

³⁹ Article 2, UCPD.

⁴⁰ Cartwright P. and Hyde R., Virtual coercion and the vulnerable consumer: 'loot boxes' as aggressive commercial practices, Legal Studies 42, pp. 555-575, University of Nottingham, Nottingham, UK, 15.01.2022, available at: <https://doi.org/10.1017/lst.2022.7>.

⁴¹ Cartwright P. and Hyde R., Virtual coercion and the vulnerable consumer: 'loot boxes' as aggressive commercial practices, Legal Studies 42, pp. 555-575, University of Nottingham, Nottingham, UK, 15.01.2022, available at: <https://doi.org/10.1017/lst.2022.7>.

their inferred cognitive makeup⁴². For example, suppose a trader misuses knowledge of a consumer's vulnerable circumstances by offering products on instalment credit to financially vulnerable or indebted consumers. In that case, that may constitute an aggressive commercial practice based on '**undue influence**' (see case study on behavioural/personalised advertising in Annex 5).

Aggressive commercial practices in the digital environment also include cases of **dynamic pricing** that take place during the transaction (whereby a trader raises the price for a product during the booking process after the consumer has put it into their digital shopping cart or proceeds to payment, without giving the consumer reasonable time to complete the transaction), which one can consider **harassment**.

The Netherlands Authority for Consumers and Markets (ACM) has Guidelines on boundaries of online persuasion to protect the online consumer⁴³. Suppose the techniques that traders that sell games use to boost sales of products with microtransactions put such pressure on consumers that they can no longer make an informed choice. In that case, ACM deems these to constitute '**undue pressure**' and an aggressive commercial practice. An example they mention is the use of algorithms that determine the price, offer, or time based on data concerning the specific psychological vulnerabilities of certain players.

Therefore, many online commercial practices fall under the three 'aggressive' category types.

RQ2(2) – Are there any new aggressive online commercial practices that challenge the UCPD's effectiveness? Which types of traders and market sectors are making most use of such practices? Are there any differences between EU Member States or regions or EU and non-EU traders?

Aggressive commercial practices in the digital environment have been a growing concern for the European Commission. In its 2013 communication on the application of the UCPD⁴⁴, the Commission highlighted that a few Member States signalled **aggressive practices targeting children in online games**. More recently, consumer organisations have also criticised the games industry for its aggressiveness, especially since **children** are a significant and vulnerable audience⁴⁵. This evolution and the market highlights below make this sector a prominent one in the use of aggressive commercial practices:

- 52% of the population (aged 6-64) play video games, and the number of players has increased from 118.3 million in 2020 to 124.8 million in 2021 on all platforms (mobile devices, consoles, and PCs).
- On average, Europeans spend 9 hours per week playing video games.

The Commission's 2020 New Consumer Agenda⁴⁶ also highlights the **exposure of children and minors to aggressive commercial practices online**. Moreover, **all sectors use aggressive commercial practices**. According to a survey that BEUC commissioned, consumers are familiar with firms pressuring them to purchase. 61% of respondents sometimes felt pressured by a website or app to buy. For almost one-third of the respondents (29%), this happens half of the time or more frequently. Nearly half (40%) ended up buying

⁴² Johann Laux, Sandra Wachter, and Brent Mittelstadt, Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice, Common Market Law Review, 58(3), 09.04.2021, Available at: <https://ssrn.com/abstract=3822962>.

⁴³ ACM, Guidelines – Protection of the online consumer – Boundaries of online persuasion.

⁴⁴ European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of the Unfair Commercial Practices Directives – Achieving a high level of consumer protection – Building trust in the Internal Market, Brussels, 14.03.2013.

⁴⁵ UFC-Que Choisir, Jeux vidéo – L'industrie doit cesser de se jouer de vous, 01.06.2022.

⁴⁶ European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the New Consumer Agenda – Strengthening consumer resilience for sustainable recovery, Brussels, 13.11.2020.

products or services they did not mean to⁴⁷. While they are **not specific to the digital environment**, it is essential to recognise that **the scale of the problem has increased with the development of the online market economy**.

The exposure of children to, for instance, aggressive marketing of food, to alcohol ads or to influencers promoting vaping, is also a point of increasing concern. Surveys⁴⁸ by BEUC show that children are massively targeted by unhealthy food adds and recognise the strong influence of marketing of unhealthy foods over children's eating behaviour. According to the recent scientific opinion "Towards Sustainable Food consumption" prepared by Scientific Advice Mechanism (SAM), advertising unhealthy diets and foods that are poor 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.⁴⁹

Online traders have more extensive access to personal data than offline, giving them more opportunities to develop or use aggressive commercial practices. It means that there is a **power asymmetry between traders and consumers**. BEUC uses the term "digital asymmetry" to describe this power imbalance between data-empowered traders and consumers. Online traders control the choice architecture and the information presented to the consumer. As a result, nearly all services consumers encounter in the digital environment use insights from their previous online searches. Even if consumers are aware of the personalisation of their online experience, they may not realise the extent of it or the distortion it introduces into their view of the market and the choices they make. This resulting state of vulnerability applies to all online consumers⁵⁰ (see case study on consumer vulnerability). Traders may use some information in a way that might affect the consumer psychologically, which can, therefore, amount to coercion or undue influence⁵¹. According to the survey that BEUC commissioned, consumers generally do not welcome AI technologies that seek to evoke their emotional responses (an example would be recommender systems suggesting disturbing content to capture attention). Almost six in ten people (59%) find it unfair for apps and websites to use artificial intelligence to trigger strong emotional responses from users, such as fear or anger. Less than one in five consider it fair that ads target them based on their lives or vulnerabilities.⁵²

Therefore, the nature of the problematic practices varies significantly as the digital environment allows traders to develop many such techniques.

2.1.4 Subscriptions

RQ3 – What are the specific modalities for consumers in relation to the length of subscription contracts for digital services and their automatic renewal?

⁴⁷ BEUC commissioned a survey analysed by an independent research and consulting firm (Open Evidence). It collected the opinions of 4 929 respondents through an online questionnaire across eight EU countries (France, Germany, Italy, Lithuania, Poland, Romania, Spain, and Sweden) throughout February and March 2023. The questionnaire comprised more than 20 questions with slightly over 600 respondents per country. Samples mimicked the proportion of gender and age in each country to be considered representative of the population. The survey was limited to adult respondents (older than 18 years old). BEUC, Connected, but unfairly treated – Consumer survey results on the fairness of the online environment, 09.2023.

⁴⁸ <https://www.beuc.eu/press-releases/children-massively-targeted-unhealthy-food-ads-consumer-groups-snapshot-exposes>

⁴⁹ European Commission, Directorate-General for Research and Innovation, Group of Chief Scientific Advisors, Towards sustainable food consumption – Promoting healthy, affordable and sustainable food consumption choices, Publications Office of the European Union, 2023, <https://data.europa.eu/doi/10.2777/29369>, p.40

⁵⁰ BEUC, EU Consumer Protection 2.0, 'Protecting fairness and consumer choice in a digital economy', 10.02.2022.

⁵¹ European Commission, Directorate-General for Justice and Consumers, Mascarenhas de Ataíde, R., Barroso Rodrigues, A., De Araujo Meirelles Magalhães, F., et al., Consumer protection in the European Union: challenges and opportunities, Publications Office of the European Union, 2023, <https://data.europa.eu/doi/10.2838/457132>.

⁵² BEUC commissioned a survey and analysed by an independent research and consulting firm (Open Evidence). It collected the opinions of 4 929 respondents through an online questionnaire across eight EU countries (France, Germany, Italy, Lithuania, Poland, Romania, Spain, and Sweden) throughout February and March 2023. The questionnaire comprised more than 20 questions with slightly over 600 respondents per country. Samples mimicked the proportion of gender and age in each country to be considered representative of the population. The survey was limited to adult respondents (older than 18 years old). BEUC, Connected, but unfairly treated – Consumer survey results on the fairness of the online environment, 09.2023.

RQ4 – Are subscriptions adequately addressed in the Unfair Commercial Practices Directive (UCPD), the Consumer Rights Directive (CRD) and other EU laws?

A case study on subscriptions was undertaken and is available in the annex, where the issues are analysed in further detail. Below, an overview of the problem is provided, focusing on the technical difficulty for consumers to terminate a contract for digital content or services (subscription traps), free trials, and trader approaches to termination by the consumer of contracts including technical means including the frequency of subscription reminders.

Subscription traps

Issues relating to subscriptions have been of growing concern for European authorities at the EU and member state level in recent years. The CPC Network in particular has reported a frequent fraudulent online trap consisting of presenting products for a free trial or at a very low cost, but hiding in the small prints that taking up such an offer would lead to a subscription with recurring payments.⁵³ While there are general protections in the **UCPD** against unfair, misleading and/ or aggressive practices in online subscriptions, the problem of subscription traps remains prevalent, with many complaints by consumers that they have been charged for subscriptions they no longer wanted. A major study on subscription traps in 2016 for the Commission's DG JUST confirmed their prevalence.⁵⁴

Some regulators have taken the view that dark patterns are prevalent in subscriptions leading consumers to become trapped. Their perception is that enforcement by itself was inadequate to address the problem. Regarding the prevention of subscription traps, the general principles clauses should in theory protect consumers as business practices by law should avoid unfairness. However, in practice, various studies have found that subscription traps continue to be a problem. Beyond the UCPD provisions, the guidance makes clear that it should be easy to exit from, as to enter into a contract, a principle already incorporated as a legal provision in other EU law e.g. the DMA's Art. 6(6), which refers to the possibility of easy switching between, and subscription to, different software applications and services.

Free trials

A further challenge relates to free trials. These are problematic when consumers are charged at the end of a free trial without being adequately informed, through pre-contractual information provision or subsequent reminder notifications, that the trial would automatically convert into a paid subscription. The results from the website sweeps (Annex 4) suggest that problems with free trials remain an issue for EU consumers. For example, in practice, consumers have to provide payment information in 39.1% of cases where a trial is offered. Although from an industry perspective, this is argued to be a valid business practice, which can for example serve as a proxy for age verification, it nonetheless allows the possibility for consumers to be charged without their express consent at the point of conversion.

Additionally, it was found in the sweeps that all free trial subscriptions would automatically turn into a paid subscription if no action is taken by the user at the end of the free trial. This can be problematic if insufficient pre-contractual information was provided at the point of signing up for the free trial in the first place that it would convert into a paid-for subscription subsequently. Both the fairness of this mechanism for consumers, and burden placed on consumers to actively opt-out before a paid subscription begins (especially in cases where payment details have already been provided and advanced warning is not provided) should be addressed more explicitly as problematic practices.

Studies at EU level involving behavioural experiments for free trials have been conducted to explore how far the provision of different types of information affected the likelihood that respondents would sign up for a free trial and whether consumers noticed the subscription fee

⁵³ [Consumer frequent traps and scams - European Commission \(europa.eu\)](#)

⁵⁴ European Commission, Directorate-General for Justice and Consumers (2016), Study on online subscription traps.

and cancellation terms. Among the findings from a study by Rand, for instance, were that:

- 71 per cent of free trials for cosmetics and 69 per cent for health supplements were found to pass the details of consumers to others.
- The trader ID was not specified or unclear for 61 per cent of free trials for health supplements and 51 per cent for cosmetics.
- The procedure to withdraw was not specified or unclear for 56 per cent of the free trials for health supplements and cosmetics.

A further finding was that "overconfidence in remembering to cancel a free trial is likely to contribute to the success of subscription traps".

Frequency of subscription reminders

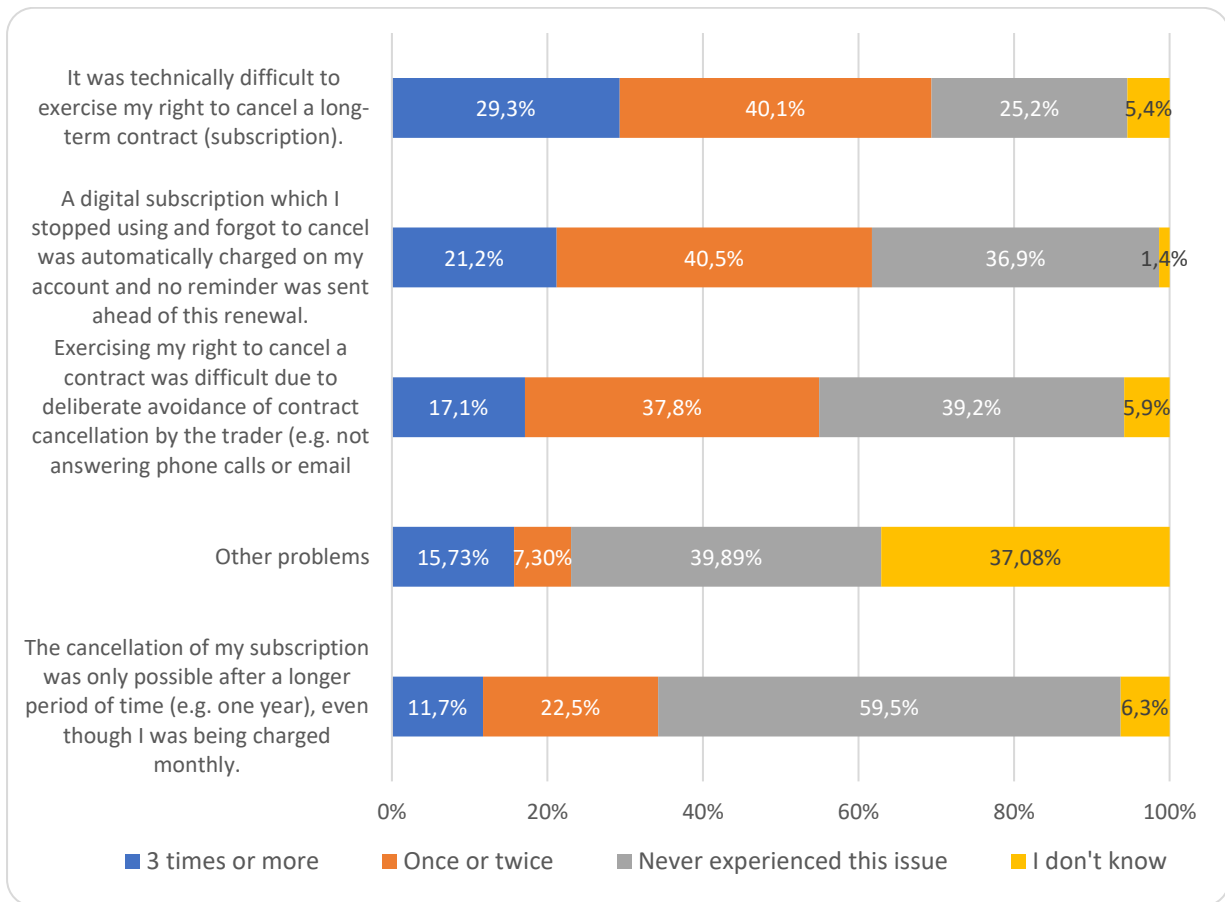
Traders had concerns that not all consumers would appreciate receiving regular monthly reminders. Whilst good practices relating to automatic subscription reminders were identified among many traders, platforms and app stores, practices vary.

In third countries, such as in the UK's 2023 Digital Markets and Competition Bill, there is proposed new legislation on subscriptions, for instance, mandating sending out auto-reminders ahead of renewals and ensuring that it is not made unfairly difficult to cancel a contract.

The CRD sets out requirements for providers of subscription services, namely that they must ensure the **transparent and intelligible provision of contractual information both prior to and throughout the duration of a contract period**. The necessary steps and means of withdrawal from any such contract must be likewise apparent to the consumer, this must also be communicated to the consumer ahead of any potential automatic renewal.

The public consultation enquired about the prevalence of different problems relevant to online subscriptions, covering issues such as subscription traps in relation to subscriptions subject to automatic renewal, free trials converting into paid subscriptions without adequate cancellation information in advance of the renewal or sufficient pre-contractual information that when signing up to a free trial, the consumer was in effect entering into a contract, and whether reminders are provided ahead of automatic renewals:

Q4 'In the past 12 months, have you experienced any of the following?' (n=222) (Relating to online subscriptions).



Source: public consultation

A lack of clear procedure for cancelling digital subscriptions was reported in the public consultation as being particularly troublesome for consumers, with 69.4% having faced technical difficulty in exercising their right to cancel a long-term contract. Similarly, potential misleading bad practice was reported by 61.7% of respondents who did not receive any notification reminder ahead of a subscription renewal being actioned. The experience of public respondents is supported also by the findings of the website sweeps conducted for this report (Annex 4). The sweeps found that in relation to the right of withdrawal, more could be done by the majority of traders to strengthen the clarity of information relating to withdrawal rights and the perceived difficulty of the cancellation/withdrawal procedure itself. Only 41.7% of websites in the sweep were considered by researchers as having presented information on the right of withdrawal clearly or very clearly. In relation to the cost and renewal of subscriptions, the sweeps found that precontractual information was generally presented clearly (61.7% of websites clearly presented costs, 54.2% clearly presented renewal information). Relating to a trader's procedure regarding reminders or notifications where subscriptions accounts or users are deemed inactive, the sweeps found that only 11.5% of websites clearly presented information at the pre-contractual stage, suggesting there is still room for improving this practice among traders in line with the principle of fairness by design.

In the representative 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). Moreover, 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). In addition, 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. 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.

Ability of EU legal framework to address the problem

The **adequacy of the CRD and other EU laws to address online subscription traps resulting from free trials was found to be limited**. Although the CRD contains relevant articles that apply to various digital contracts, it does not explicitly cover subscriptions as a separate category. Instead, it encompasses a wide range of digital contracts without addressing subscriptions explicitly.

While the CRD emphasises the importance of pre-contractual information, consumer consent, and the acknowledgement of payment obligations, **it lacks explicit regulations for key elements of subscriptions**. Specific aspects such as free trials, reminders for automatic renewal, and the requirement of a cancellation button are not explicitly regulated by the CRD. Further issues highlighted by the consumer survey suggest also that the CRD does not currently address issues sufficiently, with a majority (of 6362) respondents reporting having previously had issues with purchasing digital content/services including subscriptions, as they had not been adequately informed prior to purchase about limitations on usage, including the number of times or duration during which access was permitted (51%), or about additional purchase requirements for certain features (59%).

On the issue of hidden costs, or *de facto* hidden costs in terms of hidden limitations and stipulations placed on the use of products and services with a subscription, the Commission and the CPC Network have found that problems remain (e.g. when consumers are billed less upfront and then the recurring payment is much higher).⁵⁵

Some progress has nonetheless been made in strengthening the transparency of recurring payments for subscriptions, for instance through a 2021 CPC Network action concerning credit card companies that aimed to strengthen compliance with the Payment Services Directive and Unfair Commercial Practices Directive.

The role of credit card companies in strengthening transparency about forthcoming subscription-related transactions should also be highlighted as an example of good practice. Informing consumers in advance of them making a decision that enables them to make informed choices and to remain in control by ensuring they receive information ahead of a subscription renewal such that they can consider whether they wish to renew or cancel before the renewal date. In 2022 and 2023, American Express, Mastercard and Visa have tightened their rules for merchants to avoid consumers falling into subscription traps. For instance:

⁵⁵ Hidden costs of subscriptions and research by CPC Network on subscription traps and scams (2020) https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en

Mastercard: Merchants must now disclose the subscription terms simultaneously with a request for card credentials. The disclosure must include:

- 1) The price that will be billed;
- 2) The frequency of the billing;
- 3) If relevant, terms of the trial, including any initial charges, the length of the trial period, and the price and frequency of the subsequent subscription.

VISA: From 2023 on, merchants will need to ensure that the length of any trial period, introductory offer, or promotional period, as well as the transaction(s) amount(s) is clearly displayed on both the webpage where the card credentials is requested and entered, and on the checkout screen. The transaction(s) amount(s) to be clearly displayed include specifically the amount due at the time of purchase (even if zero), and the amount and fixed date or interval due for each recurring transaction.

American Express: Merchants must now clearly disclose all material terms of the offer including, if applicable, the fact that Recurring Billing Charges will continue until the option is cancelled by the Card member. If this includes an introductory offer, they should send the Card member a reminder notification in writing before submitting the first Recurring Billing Charge, that allows the Card member a reasonable amount of time to cancel.

In the interview programme, whereas consumer associations were in favour of prohibiting traders from collecting payments data during free trials, trader associations expressed concerns that this would not be favourable for consumers as it could risk traders becoming more reluctant to offer free trials if there is no automatic conversion into a paid contract following the trial, given low potential conversion rates. However, a legal academic interviewed from ELI pointed out (as also reflected in the ELI position paper on digital fairness) that there are means of striking a compromise in that even if collecting payment data for free trials were to be prohibited under EU consumer law, traders could still charge a minimum token amount allowing them to then collect payments information.

Specific aspects such as free trials, reminders for automatic renewal, and the requirement of a cancellation button are not explicitly regulated by the CRD.

Terminating a contract for digital content or services can pose technical difficulties intentionally created by traders and platforms. Traders employ tactics like complicated navigation menus, skewed wording, confusing choices, and repeated nudging. These tactics are designed to obscure and manipulate the termination process, making it challenging for consumers.

The absence of specific requirements, such as a cancellation button and clear information on automatic renewal and reminders, contributes to the difficulties faced by consumers when attempting to terminate contracts. Some traders may further complicate the process by allowing termination only through phone calls or chat interactions with sales representatives trained to dissuade consumers from cancelling. These approaches aim to delay and obfuscate the termination process, discouraging consumers and making it more time-consuming.

Traders use various technical means, including complicated navigation menus and confusing choices, to deter consumers from terminating contracts. The frequency with which such technical means are employed may vary among different traders and platforms. However, the exact frequency of these technical means is not specified in the provided information.

National laws on online subscriptions have been introduced in Germany, France and in Belgium. These pertain to different aspects of subscriptions as explained below:

- **Germany**, state legislation has taken this further specifically in relation to online subscriptions, by introducing a mandatory clear tick-box option for the cancellation of subscriptions by requiring a cancellation button on websites. On 1 March 2022, the first part of the “Fair Consumer Contracts Act” in Germany came into force. Among the

important changes that the legislation brings is the auto-renewal of subscription contracts. The automatic renewal of subscriptions will only be possible if the contract is extended for an indefinite period, i.e. without a further minimum term. Consumers must also 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. Before the reform, auto-renewal clauses could extend the contract for a new term of one year and the notice period before the end of the initial period could be three months.

- **France** introduced rules on online subscriptions in 2022. According to the "Châtel" law, consumers must be informed 1 to 3 months before the renewal date, of the forthcoming renewal of their contract and of the cancellation modalities by a letter or a dedicated e-mail (art. L215-1 and according to the French Consumer Code). However, this rule does not apply to all types of subscriptions as it depends on their duration. The new provisions allow subscribers to cancel more easily and at less cost if they cancel prior to their fixed term contract expiring (e.g. a mobile phone contract). Furthermore, Article L. 215-1-1 of Consumer Code provides that the consumer is entitled to terminate their contract online and at no cost by using a button labelled "terminate the contract" (or equivalent) which is easily and directly accessible on the online interface which allows the consumer to conclude a contract.
- **Belgium** – specific guidelines clarify the form and content of fixed-term service contracts that contain a tacit renewal clause. Belgium has uniquely 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. Additionally, after the first tacit renewal, the consumer has the right to terminate the contract without compensation, provided they give a notice period of two months or less. The guidelines established for fixed-term service contracts with a tacit renewal clause also apply to sales contracts for both goods and services, such as fitted kitchens and tiling. However, fixed-term contracts for the delivery of goods, like magazine subscriptions and book clubs, are not included in this provision. However, there is an option to expand this rule to certain types of goods via a royal decree.

The extent to which tools such as the cancellation button in Germany could also be a useful tool at EU level to ensure ease of cancellation in the same way that the new right of withdrawal button has made it easier to withdraw from a contract (through a 2023 amendment to the CRD) is being debated among stakeholders.

In terms of feedback, there were divergent views among different stakeholders, especially between consumer and trader associations. Consumer associations stated that:

- It remains too difficult to cancel subscriptions, with too many steps involved in the cancellation procedure and/ or traders making it difficult to exit from a subscription without calling a call centre or talking to a human via chat box.
- The principle outlined in the UCPD guidance that it should be as easy to exit from as to enter into a subscription is often not adhered to by traders.
- Some consumer associations regarded the requirement to provide credit card details as being a barrier to the uptake of digital products and services, and this may limit the full potential of the digital single market. However, traders were concerned that no longer requiring payment details has certain disadvantages e.g. making it more difficult to check whether consumers are minors and the high costs of the provision of free trials given high cancellation rates are common and this represents a business cost.

- The main concern among some trader associations (and legal academics) is that the requirements in German legislation on cancellation buttons are considered too prescriptive from a design/user interface perspective. The button was seen as only being suitable for e-commerce websites and not for other platforms or different types of digital devices (e.g. screenless devices such as voice assistants are common). Platforms were keen to highlight that they already provide cancellation options via device and application settings.
- Further concerns were that beyond the RoW period, cancellation rights currently are in the period leading up to an annual renewal and there were considerations around how a cancellation button can be integrated within an interface given that for some contracts, the cancellation period is quite short within an annual contract.

By **making cancellation processes intentionally arduous** (whether by more obvious design practices or through subliminal algorithmic and behavioural approaches), unscrupulous traders can undermine consumers' autonomy and ability to freely exercise their rights. A popular view shared by traders consulted is the primary need to promote digital literacy and consumer awareness ahead of stricter regulatory burdens on subscription providers. Educating consumers about their rights, highlighting potential pitfalls of online subscriptions, and fostering critical thinking skills can empower individuals to make informed choices and resist manipulative practices. However, consumer protection authorities and scientific research suggests that it is unreasonable to expect consumer education to be sufficient in overcoming the information asymmetry and behavioural profiling of algorithmically-driven dark patterns and deceptive design.

Evidence was found of **some dubious practices in automatic subscriptions**, such as heavily discounted initial promotional prices, with prices being significantly increased in subsequent automatic monthly or annual renewals without forewarning or adequate consent.

Practices such as the potential use of **consumer data to personalise and target subscription offers** continue to raise concerns. Traders may anonymise and legitimately leverage data analytics and algorithms to identify consumers' preferences, able to trace and predict behaviour patterns and vulnerabilities, tailoring subscription packages to maximise sign-ups and make the cancellation process more complex. By manipulating user interfaces, obscuring important information, and employing misleading pricing strategies, traders can create a sense of urgency or fear of missing out, trapping consumers into long-term commitments without fully understanding the terms and conditions. Additionally, data collected through the public consultation highlights that almost 69.4% of consumers reported feeling that digital subscriptions were at least sometimes difficult to cancel, with 61.7% further attesting that they had been automatically charged for a subscription without receiving any reminder about the renewal.

Subscription traps

Free trials

- **Consent needs to be active not passive.** Many free trials automatically convert into paid subscriptions with only passive consent and/ or without any or adequate pre-contractual information being provided when consumers sign up for the free trial making it clear that the consumer is entering into a contract (unless they cancel before the free trial period ends) leading to consumers perceiving they had been tricked into a paid subscription.
- **Requirements to provide credit card details upfront may deter some consumers from signing up to a free trial.** However, this is difficult to legislate given the law of unintended consequences as credit card details are used for checking age and identity and there may also be reluctance among traders to offer free trials if the subsequent contract is not part of the free trial with the consumer having the right of cancellation.

Subscription traps and reminders

- **Dark patterns remain a problem in the design of website interfaces and hinder consumers in cancelling subscriptions leading to subscription traps.** Procedures for cancelling are overly cumbersome and should be simplified.
- Some traders still **do not send out reminders regarding subscription renewals**, or send a reminder, but fail to inform about key changes to the contract which mean that consumers have a new right of withdrawal upon substantive changes to the terms and conditions.

RQ5 – What technical problems do consumers face when they exercise the right of withdrawal (RoW) from the contracts for digital content or services?

RQ6 – To what extent are there problems in exercising cancellation rights?

Sub-questions considered in responding to this RQ were:

- What are the main approaches followed by traders with respect to the procedure for exercise of the right of withdrawal?
- What is the effect of the technical means proposed by traders for the exercise of the right of withdrawal, and of the design of user interface? Are these problems adequately addressed by the CRD?

As discussed above, traders adopt various approaches to impede the exercise of the right of withdrawal, such as exercising the RoW by clicking a button on a website, sending an email or making a phone call. Some methods are easier for consumers to exercise their RoW than others.

By offering only phone-based cancellation methods, traders introduce sales techniques to discourage consumers from exercising their RoW. The aim is to prolong the process and make it time-consuming compared to a simple automatic RoW button, which would provide a neutral option for withdrawal. This approach exploits consumers' reluctance to engage in lengthy discussions and deters them from cancelling subscriptions or services.

Consumer experiences reveal several technical obstacles that hinder the exercise of the right of withdrawal (RoW). Traders employ tactics such as “sneaking,” where information is hidden, disguised, or delayed, making it difficult for consumers to find the necessary details for withdrawal. Additionally, traders engage in “obstruction” by deliberately making the cancellation process more cumbersome than necessary. For instance, requiring cancellations to be made exclusively through phone calls serves to dissuade consumers from cancelling and prolongs the procedure. These technical challenges create confusion, complicate navigation, and deter consumers from effectively exercising their right of withdrawal.

The design of user interfaces plays a critical role in facilitating or hindering the exercise of the RoW. However, this problem has recently been addressed. As a result of the distance marketing of consumer financial services (DMFSD) review, a RoW button⁵⁶ will be introduced in the CRD for all distance contracts.

The design of user interfaces also plays a key role in facilitating or hindering the exercise of cancellation rights beyond the 14-day right of withdrawal. This raises the issue as to whether there is a need to strengthen consumer rights regarding the ease of cancellation such that the general principle already included in the UCPD guidance that it should be as easy to exit from a contract as to enter into it becomes a reality across digital markets and services. As per the more detailed assessment provided in the case study on online subscriptions, a cancellation button could be useful to facilitate contract cancellation provided that the approach is not

⁵⁶ <https://www.finance-watch.org/going-further-to-make-the-online-financial-services-market-safer-and-fairer-for-europeans/>

overly-prescriptive (recognising that there are different types of design interfaces across different types of traders (e.g. e-commerce websites, screenless devices, platforms, apps). **Further suggestions regarding the cancellation button are made under relevance in the section on the possible solutions identified to address dark patterns.**

While the CRD establishes fundamental consumer protection standards across the EU, it falls short in explicitly addressing the technical challenges consumers face when exercising cancellation rights. The Directive primarily focuses on disclosure requirements, transparency, and general rules for distance contracts, providing a baseline for consumer rights. However, the CRD does not offer specific guidance or regulations concerning the aforementioned technical problems, trader approaches, and user interface design issues. As a result, consumers may find it challenging to effectively exercise their cancellation rights in the digital realm. The lack of a requirement in the CRD and in the UCPD to ensure fairness by design from the outset may have contributed to the opaqueness in cancellation procedures of some digital services and products (and offline products and services signed up to online).

2.1.5 Personalised advertising

RQ7 – 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 already sufficiently addressed by existing legislation?

Surveys suggest that consumers are concerned that they are being targeted, and that content that they see is being tailored without their knowledge or permission.⁵⁷ Moreover, even if information is provided to inform consumers that their data is being used for personalised advertising, it may not be easy to understand how their data is being used to tailor content⁵⁸ or to opt out from personalisation practices.⁵⁹

Respondents were asked whether they had ever had a situation in the previous 12 months regarding the perceived misuse (or unfair use) of their personal data to personalise commercial offers. The results are shown below:

Table 2-2 – In the past 12 months, have you experienced any of the following problems online? My personal data was misused (or used unfairly) to personalise commercial offers (e.g. the company seemed to use information about my specific weaknesses and vulnerabilities when showing me personalised content).

Response options	Number	%
3 times or more	100	45.1%
Once or twice	65	29.3%
Never experienced this issue	39	17.5%
I don't know	18	8.1%
Grand Total	222	100%

Source: Public consultation

It is notable that around three-quarters of respondents to the public consultation said that within the last 12 months they had experienced situations where their personal data was

⁵⁷ In the 2023 Consumer Conditions survey, 70% of respondents reported that they were concerned about the use and sharing of their personal data in the context of online advertising, and more than half expressed concerns about the installation of cookies and collection of online data. This is corroborated in a consumer research report funded by the digital advertising industry “Your online voices”, 2022, a conversation with consumers in France, Germany, Belgium, and Latvia available at: <https://edaa.eu/your-online-voices-your-voice-choice/>

⁵⁸ A 2018 study for DG Justice: BEHAVIOURAL STUDY ON ADVERTISING AND MARKETING PRACTICES IN ONLINE SOCIAL MEDIA, (2018) GfK for the EC DG JUST highlights a concern that “a majority of online social media users are likely to unknowingly consent to their personal data being used [for targeting] due to complex terms and conditions that they do not understand or take the time to read

⁵⁹ 37% of consumers responding to the 2022 Consumer Conditions survey noted that a key concern about online advertising was that they could not opt-out or refuse to receive it.

misused or used unfairly to personalise commercial offers (45.1% said this occurred 3 or more times, and 29.3% once or twice). Furthermore, in a follow-up question, 11% of respondents considered that this was the single most serious problem they had experienced online in the past 12 months.

Furthermore, the representative consumer survey found that:

- 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**. The results were particularly high for consumers who considered themselves to be 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 cohorts (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 age cohort (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 **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.

These concerns persist despite the fact that EU rules have been put in place through *inter alia* the GDPR and DSA which establish the boundaries of the collection and processing of personal data for personalisation purposes,⁶⁰ prohibit online platforms from presenting targeted advertising to minors or based on sensitive data, and require consent for data storage on an individual's device (e.g. through cookies under the e-Privacy Directive)⁶¹ and require transparency regarding profiling⁶² and the use of data for personalisation purposes⁶³ as well as transparency by online platforms (at the time of display) regarding parameters used for personalised advertising,⁶⁴ and at the time of contract (for distance or off-premises contracts)

⁶⁰ Processing personal data for the purposes of personalised advertising in a manner which is unfair or is not clearly explained amounts to a breach of the GDPR. Article 6 GDPR limits the legitimate processing of personal data to six grounds, with consent being a key condition regarding personalisation for advertising or commercial purposes (as per EDPB Guidelines). The DSA (Article 26) goes further in stipulating that providers of *online platforms* should not present advertisements to minors or based on profiling which relies on special categories of personal data including data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, data concerning health or a natural person's sex life or sexual orientation.

⁶¹ The ePrivacy Directive requires the user's consent when cookies or other forms of accessing and storing information on an individual's device (e.g., tablet or smartphone) are used.

⁶² The GDPR requires that the data subject be informed when the data controller uses profiling techniques

⁶³ Article 6 GDPR requires that data subjects are given relevant information on the purposes for which data is processed

⁶⁴ The DSA (Article 26) stipulates that online platforms that present advertisements on their online interfaces must ensure that for each specific ad presented to each recipient the latter is able to identify *inter alia* that the information is an advertisement and the main parameters used to determine the recipient to whom the advertisement is presented, and, where applicable, how to change those parameters.

regarding personalised pricing.⁶⁵ Furthermore, personalised advertising, prices and offers which constitute “aggressive practices” (in that they materially distort or are likely to distort the economic behaviour of an average or vulnerable customer) could be prohibited under the UCPD, based on a case-by-case assessment.

In the targeted consultation, respondents were asked how far they perceived that EU consumer law Directives contributed to ensuring the transparency and fairness of personalisation practices.

Table 2-3 – To what extent have the EU consumer law Directives contributed towards achieving the objectives of ensuring the transparency and fairness of personalisation practices (e.g. personalised advertising, pricing, offers, ranking, recommendations)?

Response options	Number	%
To a great extent	41	30.6%
To a moderate extent	51	38.1%
To a small extent	23	17.2%
Not at all	19	14.1%
Grand Total	134	100%

Source: targeted consultation

68.7% agreed to a great or a moderate extent. However, the respondents were more skewed towards traders and business associations. A perceived lack of effective enforcement of existing provisions in the GDPR and e-Privacy Directive may be partly responsible for the continued concerns of consumers. For example, in addition to cases where the required information is not provided, the use of dark patterns (display of “choices” in a manner which seeks to influence the consumer) in combination with profiling can limit the degree to which consumers give consent to the use of their data for personalisation freely as well as “nudging” them towards certain offers or contracts.⁶⁶

The lack of effectiveness could also partly be explained by the fact that provisions which require transparency about personalisation *at the time of display / contract* have only been recently introduced including changes to the CRD to require information about personalised pricing and DSA provisions to require information about personalised advertising. Additional measures requiring gatekeeper platforms to make available a less personalised alternative under the DMA must be implemented by gatekeepers from 7 March 2024.

It is possible that consumers’ concerns could be addressed through more proactive enforcement of existing rules coupled with effective implementation of the existing rules, including in the DSA. However, there are also reasons to believe that enforcement may still be challenging to achieve and potentially insufficient to address the core concerns of consumers:

- Existing rules stem from a range of different horizontal, platform and sector-specific legal instruments and may (especially for smaller traders) be difficult to understand. They may also be difficult to apply due to the range of different enforcement bodies involved at EU and national level (e.g. European Commission for the DMA and for

⁶⁵ The CRD, as amended by the Modernisation Directive includes an additional requirement (Art 4(4)(a)(ii) that “before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with information in a clear and comprehensible manner... that the price was personalised on the basis of automated decision-making”.

⁶⁶ Based on a behavioural experiment testing consumers’ reactions to dark patterns and manipulative personalisation, a 2022 study ‘Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation, study by Open Evidence, LSE, BS and BDI Research for the EU Commission, April 2022) found that personalisation has a reinforcing effect combined with dark patterns (toying with emotions) leading to a higher (+4 percentage points) preference inconsistency.

VLOPs and VLOSEs in the DSA, national data protection authorities and consumer protection authorities for the GDPR and UCPD, and “Digital Service Co-ordinators” for the DSA).

- While the UCPD and GDPR apply to substantially all cases, the additional measures which have been applied to address concerns specific to personalisation contain gaps whereby some rules apply to certain situations or categories of actors or services, but not others. For example:
 - The DSA (Art. 26) stipulates that providers of online platforms should not present advertisements based on profiling which relies on special categories of personal data including data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, data concerning health or a natural person’s sex life or sexual orientation. However, it refers only to advertising (and not other forms of personalisation) and does not apply to traders other than online platforms. It also does not cover other categories of sensitive data that may relate to consumer vulnerabilities (e.g. financial situation, gambling history, negative mood).
 - CRD measures regarding transparency for pricing made using automated decision-making only apply to distance contracts (and not contracts entered into by other means), and do not extend to other forms of personalisation (such as personalisation of the offer, which could result in nudging towards specific pricing categories). Furthermore, this provision only requires minimum information (i.e. a mere declaration) about the presence of a personalised price (through the amendment made through the Modernisation Directive), and not whether this advantages or disadvantages the consumer.
 - DSA measures regarding transparency for online advertising apply to online platforms, but not other hosts of advertisements, and require transparency about the parameters used to determine the recipient specifically for advertising (but not other forms of personalisation such as personalised offers or prices). Furthermore, the DSA requirement for presenting consumers with a non-personalised version of a recommender system only applies to very large platforms and search engines.
 - DMA measures requiring the provision of a less personalised service apply only to “gatekeeper” platforms, but not other online platforms. 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.
- Behavioural experiments have found that the existing approach to addressing concerns with personalisation (which is based on consent regarding the collection of data and transparency - at the time of data collection, and increasingly at the time of display / contract) may not be fully effective in empowering consumers to choose how their data is used and whether they are subject to personalisation. The main reasons, which are further explained in the relevant case studies⁶⁷ are that:
 - A case-by-case approach to consent for the use of data for personalisation can be overwhelming for consumers, creating information overload, and leading to consent by default.
 - The increasing complexity of algorithms makes it difficult to effectively explain to consumers how profiling has been carried out and how it affects the advertising,

⁶⁷ See behavioural advertising case study in separate case study annex.

content or price displayed. This can in turn limit the effectiveness of transparency measures, and means that consumers are not adequately “informed”. This problem is likely to be exacerbated with the development of more sophisticated profiling and targeting measures making use of AI.

Concerns about the use of compromising personal data and personal characteristics and/or vulnerabilities in relation to targeted advertising were expressed in several public consultation position papers (e.g. BEUC, Consumer Council Tænkt Danmark, CCPC, UFC-Que Choisir and ELI, the European Law Institute). Another personalisation practice that many stakeholders (e.g. consumer associations, Ministries, CPAs, some legal academics) were in favour of explicitly prohibiting was the development and use of new behavioural insights software and technologies focusing on consumers’ emotions (e.g. delivering emotional insights into individual consumers’ behaviours and using manipulative practices to exploit these through personalised advertising). Such marketing approaches were seen as raising ethical considerations and undermining consumer protection. The use of such technologies to develop personalisation practices was seen as a manipulative practice by these stakeholders.

The Netherlands Authority for Consumers and Markets outlined their views in a position paper responding to the public consultation, saying that *“Personalised commercial practices should be in the economic interests of consumers, and they should not lead to discrimination or exclusion, particularly of vulnerable groups. Nor should they exploit consumer weaknesses.”*

However, some trader representative stakeholders expressed caution in that whilst they agreed that manipulative personalisation practices could be outlawed, data-driven advertising was seen as being a key element of traders’ business models in the internet era, and they argued that the GDPR plus the rules in the DSA on marketplaces and platforms regarding not using certain sensitive data is already sufficient.

The extent to which the definition of which types of personal information should or should not be used for personalised advertising is considered in the case study on personalised advertising in Annex 3. This is further analysed under “coherence”, as under the DSA, some personal characteristics cannot be used for personalised advertising by online platforms. This raises an issue as to whether similar provisions are needed within the UCPD, given that the use of sensitive personal data for personalised advertising is not addressed at all in the UCPD, but is in the DSA only for platforms, whereas the UCPD provides a backstop to ensure unfair practices are prohibited for all types of traders.

Regarding stakeholder feedback on personalised advertising, traders and their representative associations recognised the GDPR’s importance in providing the legal framework as to which types of personal data can be used for ads and which cannot because they are deemed sensitive data under the GDPR’s Art. 9(1). They did not generally perceive a problem that the UCPD does not deal with data or personalised advertising in detail, given that any unfair, misleading or aggressive use of personal data in the context of B2C would fall under the general principles-based clauses of the Directive, which are already applied in conjunction with the GDPR’s provisions.

However, some consumer associations and some national Ministries and CPAs viewed the lack of any explicit attention to certain aspects of the use of personal data, including sensitive data and psychographic profiling, as causing legal uncertainty, especially as the same stakeholder types viewed this type of profiling as being unfair. Some stakeholders called for this type of personalised advertising to be banned outright. For instance, BEUC advocated in its position paper that the *“use of psychographic profiling for price personalisation should be prohibited; Personalisation practices should be rendered fair and empowering to consumers”*. This raises a question as to whether to ensure regulatory alignment regarding the new restrictions in the DSA and whether consumers should be given more control and a clearer possibility of either opting in or out of personalised advertising in future.

Some EU trader associations, such as e-Commerce Europe, independent retailers Europe, raised concerns about potentially regulating personalised advertising and pricing as they pointed out that consumers are demanding personalisation, and that this benefits consumers in terms of more relevant choices, better deals and discounts for products based on their previous purchasing history etc.

Some of the global tech players interviewed for the personal advertising case study made it clear that they did not use psychographic profiling although they did not state if they were explicitly in favour of it being prohibited. Regarding the use of personal data more generally, however, they made it clear that they had concerns regarding further regulation on the use of personal data as many business models in digital markets and services are premised on the provision of free services in exchange for the use of personal data, often for advertising-based models, although with evidence that there is a transition away from advertising-based models alone towards subscription-based models (see subscriptions case study).

If all behavioural data were to be banned from being used to target ads to users, some traders expressed concerns that this could be a step too far, as consumers express preferences for personalised advertising - or at least – do not presently opt out of such advertising frequently when given the opportunity currently (e.g. online platforms through the DSA). Whilst no data estimates were available, major global online platforms interviewed did not give the impression there was strong demand to opt-out but agreed that consumers should have the choice to do so should they so wish.

Progress in improving transparency regarding the use of personal data and information for advertising purposes was highlighted by the Dutch Consumer and Markets Authority who stated that greater transparency (including through the MD) has helped to address information and power imbalances between consumer and businesses. “Businesses can rely on extensive customer data, psychological insights and AI applications to optimise sales architectures for conversion, using their granular knowledge about customers and their cognitive biases to influence consumers’ preferences and purchasing decisions. However, to mitigate the negative effects of the imbalance, EU consumer law contains various provisions that require businesses to disclose information to consumers through transparency requirements.”

Regarding findings from the **consumer sweep on personalised advertising**, a website sweep was carried out on manipulative or opaque personalisation practices (see Annex 4 with the results) in dating and gambling services. Among the findings were that:

- 42% of ads shown were allegedly linked to exploiting consumers’ vulnerabilities.
- Most websites’ privacy policy statements state that they use marketing cookies for targeted ads; however, many websites had no ads (on some sites, the researcher stayed up to 30 minutes browsing, going through ‘likes’ and clicking through all the functionalities and still no ads).
- None of the gambling websites display ads. They display internal promotions (deal of the day, etc) but no external ads. This could be because they are restricted and monitored, but it could also be that the ads are only displayed once you start playing the games with money. For instance, some of the dating websites appear very clean and professional at the beginning with no ads displayed, but as soon as an account has been created and is used, ads start popping up, and then become more frequent.

In conclusion, existing horizontal (consumer and data protection) and sector-specific (platform related) measures relating to personalisation practices partially address consumers’ concerns. However, the consumer law framework is likely to remain only partially effective, due to the complexity of the ruleset (and consequent problems in understanding and enforcement) and challenges in devising a regime which enables consumers to provide (and withdraw) genuinely informed consent, considering complex and evolving technologies. Improvements in

enforcement and the implementation of new measures by platforms and gatekeepers (e.g. through the DSA and DMA) could improve the situation as these include more specific rules for those traders more likely to collect large datasets. However, concrete rules addressing concerns, such as the exploitation of consumer vulnerabilities beyond sensitive data, remain absent from the UCPD.

2.1.6 Personalised pricing

RQ8 – How far is online market segmentation through personalised pricing/offers unfair and, if yes, how can this can be tackled?

Different levels of personalisation (or “discrimination”) are possible.^{68 69} For example, third degree price discrimination involves setting different prices for different groups of consumers which are partitioned based on verifiable demographic characteristics such as age (e.g. setting lower prices for seniors or students, who are assumed to have lower ability to pay). Second-degree price discrimination does not rely on information about consumers but enables consumers to “self-select” by offering versions of the same product at different prices. First-degree price discrimination refers to price discrimination in which each consumer is charged according to their willingness to pay.

Third degree price discrimination, where different prices are set for distinct consumer groups is widespread, and commonly viewed as welfare enhancing. “Dynamic” pricing, whereby prices are adjusted not based on personal data but on factors which influence demand, such as time of year / day, is also considered justifiable, and is relatively common in certain industries like travel, and hospitality. Conversely, first-degree price discrimination whereby different charges are set for the same product or service, based on estimates regarding consumers’ willingness to pay is generally regarded as unfair.⁷⁰ Although these practices are widespread and long-standing in offline settings such as markets and bazaars, there is a perception that the increased depth of data available to major platforms and merchants and improvements in algorithms, alongside the potential to adapt and display personalised prices in real-time, could enable online merchants to exploit information asymmetries and vulnerabilities of individual consumers when supported by data and automated processes.

As a baseline, concerns around the lack of transparency regarding first-degree price personalisation could be addressed by informing consumers that the price has been personalised and how their data has been used to perform that personalisation. This is to some extent provided for in the amendment to the CRD that requires transparency regarding pricing that has been subject to automated decision-making. However, the CRD provisions do not apply to certain categories of contracts, e.g. healthcare, financial services, package travel and passenger transport. Moreover, as noted in relation to information regarding behavioural advertising, as data-driven algorithms become increasingly sophisticated, it may become difficult to explain to consumers how and why the price has been personalised (and the CRD does not require such explanations). Consumers may also face increased search costs (associated with checking alternative non-personalised sources of the product or service) and a narrowed perspective, if they are not also shown what the price would have been for other categories of user or in the absence of personalisation. In addition, behavioural experiments have suggested that providing more information could lead to information overload and fail to deliver better decision-making by consumers.

⁶⁸ OECD (2018): The regulation of personalised pricing in the digital era - Note by Marc Bourreau and Alexandre de Stree, DAF/COMP/WD(2018)150, 21 November 2018. See <https://ssrn.com/abstract=3312158>.

⁶⁹ [Consumer market study on online market segmentation through personalised pricing/offers in the European Union \(europa.eu\)](https://ec.europa.eu/consumer-study-on-online-market-segmentation-through-personalised-pricing/offers-in-the-european-union)

⁷⁰ This was confirmed in the Case Study regarding personalised pricing where the consumer organisations and academics interviewed considered that while presenting special offers to certain groups of consumers can be positive, first degree personalised pricing was typically viewed as unfair.

A **BEUC position paper on personalised pricing**⁷¹ published in July 2023 sheds light on how far there are outstanding consumer protection considerations around this issue. BEUC has called for a general prohibition of pricing techniques using personal data to adjust the price based on behavioural predictions made about individuals. Examples cited in the paper include: (1) *Assessing the consumers' individual willingness to pay* (2) *Using profiling to predict the likelihood of switching to a different provider* and (3) *Filtering the customer base by giving 'undesired' consumers over-inflated prices*⁷². The suggestion that manipulative approaches to pricing hidden from consumers should be prohibited on the grounds they are manipulative practices is in line with the current (but less explicit) general provisions in the UCPD prohibiting misleading practices. If such rules were to be made more explicit in future, this would help to strengthen consumer protection and prevent bad practices that exploit consumers. There could however be some practical challenges regarding the implementation of any such rules, namely the need for there to be sufficient transparency by traders regarding their internal practices and the way in which algorithms that deal with personalised pricing work to regulators and CPAs, otherwise such rules would be difficult to enforce.

Whereas the first two suggestions are somewhat less controversial, there remains complexity as regards the issue as to whether traders should be able to vary pricing in certain circumstances and to determine their own customer base, including through price discrimination. Whilst inflated prices for certain consumers could be considered as an unfair practice under the general principles-based provisions of the UCPD, depending on a case-by-case assessment of the individual facts of the case, there can be complexity in implementing such rules.

There could be some circumstances in which certain consumers are more costly to service than others, warranting some kind of price differentiation. There has been recent publicity in the UK, for example, in the online retail sector regarding the problem of a high level of returns with a minority of customers returning a disproportionate percentage of their orders. Whilst the solution has been to introduce a standard return fee for all customers (with a focus on dissuading consumers that send back returns repeatedly), some customer accounts were closed as these were loss-making. This raises an example as to how there may be differences in the costs of serving some customers⁷². Were such new rules to be implemented in future, these would need to recognise that some consumers may legitimately be charged higher prices in specific circumstances, such as geographic location, whether they send returns repeatedly etc.

Stakeholder feedback from the targeted survey as to how far there are any problems in personalised pricing is provided below.

Table 2-4 – To what extent do you agree or disagree that the following practices are problematic? Problems concerning personalised pricing

Response options	Number	%
Strongly agree	28	30.8%
Agree	30	33.0%
Disagree	16	17.6%
Strongly disagree	17	18.7%
Grand Total	91	100.0%

Source: Targeted survey

⁷¹ BEUC, 2023. <https://www.beuc.eu/position-papers/each-consumer-separate-market-beuc-position-paper-personalised-pricing>

⁷² <https://internetretailing.net/retailers-returns-price/>

The survey found that overall, 63.8% of respondents (either agreed 30.8% or strongly agreed, 33.0%) that there remain problems in relation to personalised pricing, despite the recent changes to strengthen transparency in the case of automated pricing through the MD.



Interview feedback was twofold, firstly that consumers may not be aware of the requirement under the MD indicating whether a price has been personalised, and secondly, even if they check that the price has been personalised, it is confusing for consumers to understand what the implications are.

Recently, some MEPs asked the European Commission to investigate the issue of whether **dynamic pricing** to reflect supply and demand fluctuations is a problem that could be addressed through greater consumer protection. However, dynamic pricing is clearly distinguished from personalised pricing both conceptually and legally. So long as dynamic pricing is not intentionally manipulative, e.g. scalper bots used to inflate the prices of event tickets, which was already outlawed through the Modernisation Directive, there is currently nothing illegal about adjusting prices to reflect demand/supply ratios under EU consumer law.

2.1.7 Social commerce and influencer marketing

RQ9 – What are the problems with the application of current rules on influencer marketing, taking into account enforcement cases and guidelines at national level?

Influencer marketing represents a growing share of the European economy. Despite the fact that influencers may qualify as traders, some stakeholders consider that the **absence of a legal definition for influencers** in the UCPD could create ambiguity and make it difficult to establish clear guidelines and responsibilities. As a result, it would be challenging to hold influencers accountable for misleading or deceptive content, which can have adverse effects on consumers.⁷³ There is presently a lack of a clear threshold for determining the trigger for an influencer to be defined as a professional seller and therefore be subject to the UCPD's rules on hidden advertising and other unfair practices. However, the UCPD Guidance clarifies that individuals that frequently carry out promotional activities directed at consumers on their social media accounts are likely to qualify as traders, regardless of the size of their following.

Furthermore, our research found that there is a **lack of transparency in influencer marketing**. Consumers may be unaware of the nature of influencer-brand relationships or the presence of sponsored content, leading to potential confusion and misinformation. This lack of transparency can undermine consumer trust and compromise their ability to make informed decisions. Whilst there are general rules on hidden advertising in the UCPD, and the current UCPD includes a general transparency requirement about commercial communications (Article 7(2)), there is a lack of clear **disclosure obligations** for influencers that are not considered either as traders (covered under UCPD) or as audio-visual media service/content providers (covered under AVMSD), making it challenging for consumers to differentiate between personal opinions and promotional content.

While influencers can fall under the UCPD or AVMSD, and this may cover most influencers, the uncertainty and potential for gaps in this coverage could be addressed by the introduction of a general transparency and conduct provisions for all types of influencers and their activities.⁷⁴

⁷³ Riefa, C., Clausen, C., 2019, Towards fairness in digital influencers' marketing practices, 8 (2019) EuCML Journal of European Consumer and Market Law. Available at: <https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/8.2/EuCML2019012>.

⁷⁴ Hiltunen, M., Social Media Platforms within Internal Market Construction: Patterns of Reproduction in EU Platform Law, (2022) 23(9) German Law Journal. Available at <https://ssrn.com/abstract=4285737>.

Moreover, the **cross-border nature of influencer marketing** calls for international cooperation to ensure effective regulation. As social media platforms operate globally, regulations in one jurisdiction would not be sufficient to address the challenges posed by influencers. Collaborative efforts and information sharing among regulatory bodies are crucial to developing consistent and comprehensive regulations that transcend geographical boundaries.⁷⁵ In this way, harmonised legislation and guidance at the EU level would simplify broader coordination and collaboration processes globally between the EU and other leaders in this policy area such as the US FTC.

Additionally, within the single market, harmonised legislation on influencers could potentially benefit Member States through legal certainty and the facilitation of cross-border trade. The role of influencers and their obligations as traders or audio-visual media service providers would be further clouded should Member States regulate in a non-harmonised manner influencer activities and marketing; this may amount to fragmentating the single market.

Furthermore, the **promotion of harmful products and services by influencers is a concern**. While the AVMSD regulates the advertisement of tobacco and alcohol, it does not explicitly address all products or activities which may pose a safety or health risks, leaving consumers vulnerable to potential harm. Implementing explicit restrictions on the promotion of harmful products and services would align influencer marketing practices with broader public health and safety objectives.

Regarding **enforcement cases** (see case study for further information), some national CPAs have launched actions against influencers that have not complied with existing rules on hidden advertising. For instance, the Italian CPA has taken several actions against major firms in the aviation and beauty sectors for hidden marketing in campaigns with influencers.

The UCPD applies to influencers where they engage in commercial activities, thus acting as a trader. Art. 5-9 UCPD and the accompanying UCPD guidance set out the circumstances in which influencers' actions can be considered as an unfair commercial practice within the meaning of UCPD. Additionally, the Audiovisual Media Services Directive 2010/13/EU, as revised by Directive (EU) 2018/1808 ("the AVMSD") offers additional coverage for influencers that produce on-demand audiovisual media content. AVMSD Art.9 (1) stipulates that commercial communications must be readily recognisable, with Art. 10 (1.c) highlighting the need for transparency regarding sponsored content. The AVMSD can directly require influencers, provided they classify as on-demand audiovisual media service providers, to clearly label or disclose sponsored or paid content. Among other things, Art.9 also stipulates that audiovisual commercial communications shall not include or promote any discrimination based on sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation. Furthermore, audiovisual commercial communication must not be surreptitious nor use subliminal techniques, must not encourage behaviour prejudicial to health or safety. Art.28(b) provides rules for platforms that fall under the AVMSD, placing burden upon platforms to ensure that Art.9 and 10 content and transparency requirements are upheld by content producers. Importantly, audiovisual commercial communication must respect specific rules to protect minors from advertising harms.

Regarding national legislation on influencer marketing, in most MS, this is regulated in a similar way to any other form of marketing. However, some MS have introduced, or considered introducing additional legislation at national level specifically defining and stipulating obligations for influencers and/or influencer marketing.

⁷⁵ Michaelsen, F., Collini, L. et. al., 2022, The impact of influencers on advertising and consumer protection in the Single Market, Publication for the Committee on Internal Market and Consumer Protection (IMCO), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg. Specifically, the following pages: definition of influencer (15-16), regulation (63-88), recommendations (91-96).

- **France's new Influencer Law**, adopted 9 June, 2023, defines a social media influencer and differentiates between those carrying out influencer marketing as traders and individuals for whom it is a casual hobby. Under the French law, 'influencers are now required to explicitly disclose any sponsored content or partnerships. Such disclosures should be made at the beginning of posts, ensuring that consumers are made aware about the commercial nature of content from the outset. Infringements could lead to up to two years in prison and a fine of up to €300,000.
- In **Italy**, hidden advertising is covered in the Italian consumer code, representing UCPD transposition, enforced by the consumer protection authority ACGM. Additionally, in January 2024 the media authority, Autorità per le garanzie nelle comunicazioni (AGCOM) enacted new guidelines to strengthen influencer transparency about paid promotions which aimed to ensure compliance by influencers with the provisions of the Consolidated Law on Audiovisual Media Services, covering those that have at least a million followers across social media platforms as well as an engagement rate of published content of at least two percent, as measured through reactions from users, comments or likes. The provisions concern measures regarding commercial communications, the protection of individuals fundamental rights, protection of minors and provide a mechanism for influencers to inform consumers that the content contains advertising such as promotions or sponsorship.⁷⁶
- In the **Netherlands**, the Dutch Media Act was updated and has applied from July 1st, 2022. Major influencers – defined as being above the 500,000-followers threshold and publishing at least 24 videos per year – must comply with the same advertising rules as on TV and must register with the Dutch Media Authority. Presently, the scope of the media law is limited to influencers on YouTube, Instagram and TikTok. However, an incremental approach has been proposed gradually extending to influencers with fewer followers and to more platforms. **Fines** can be imposed of up to a maximum of EUR 225,000 per violation. The media law makes an **additional distinction between advertising, sponsorship and product placement** with different labelling requirements for each.
 - Advertising, the video must clearly and visibly include the words “advertisement” or “promotion” or words of a similar meaning.
 - Product placement – the following statement is required at the beginning and end of the video, and / or commercial message: “This video/program contains product placement.”
 - Sponsoring – the following statement is required at the beginning or end of the video: “This video/program is (also) brought to you by” or “This video/program is sponsored by [the name or logo of the sponsor].”
- In **Denmark**, the Danish Marketing Practices Act (*markedsføringsloven*) was updated in on 25 November 2021.⁷⁷ The Act includes new rules in relation to influencers, such as making clear that covert advertising is not allowed, including in influencer marketing when there is commercial intent behind the post (even if the influencer has not been paid in cash but instead has

⁷⁶ New AGCOM guidelines of 10th January, 2024 on influencer marketing designed to complement the Italian transposition of the AVMSD - <https://www.agcom.it/documents/10179/32882112/Comunicato+stampa+10-01-2024/2d44dede-71b2-441f-9654-817833c4b0fe?version=1.0>

⁷⁷ The Danish Marketing Practices Act, available: [markedsfoeringsloven-lbkg-2013.pdf](https://www.markedsfoeringsloven-lbkg-2013.pdf) (forbrugerombudsmanden.dk)

received 'free gifts', discounts or other benefits from the company). However, if an influencer unilaterally decides to post a photo of a particular business or product without the business being involved in the post, no mandatory information needs to be provided together with the post if there is no commercial intent underlying the post. Part 3 of the Act also includes rules prohibiting harmful commercial practices directed at specific customers, children and young people.⁷⁸ For instance, when posting to a younger audience, influencers should avoid using aggressive tactics when posting. However, there have already been some cases against influencers under the Act relating to non-compliance.⁷⁹ The Danish Consumer Ombudsman requires that, if an enterprise enters into an agreement (written or oral) with an influencer, where the influencer mentions the enterprise or its product in any way on social media, it must be clearly indicated that such activity constitutes advertising and who the advertisement is for.

National guidance on influencer marketing has been issued by CPAs in some Member States, such as the **Netherlands** and **Sweden**. For example, the Dutch Advertising Code (Nederlandse Reclame Code, NRC) contains rules specifically for advertising via social media, the "Advertising Code for Social media & Influencer Marketing".⁸⁰ This states that traders *"must be clear about advertising, sponsoring, and product placement. They must also be considerate of children (minors) and must be clear about who they are and that they are under the supervision of the Dutch Media Authority"*⁸¹. In addition, outside of the EU, updated guidance for influencer marketing was recently issued by the regulatory body the Advertising Standards Agency (ASA) in the **UK**. For instance, consumers must always be aware when they are being advertised to, and both brands and influencers should assume responsibility for ensuring that the content makes clear any commercial ties upfront.⁸²

Overall, regulatory developments at national level pertaining to influencer marketing suggest that the current legal framework at EU level may need more specific rules. In parallel, there are alternative **ways of strengthening the effectiveness** of existing rules through more awareness-raising for influencers, such as the recent launch of an EU Influencer Legal Hub with training materials and guidance on the law for use by influencers, trade associations and others working with influencers.⁸³

BEUC published research on the issue of influencer marketing during 2023. This recommended that the promotion of illegal products and services by influencers should constitute an unfair commercial practice and be **explicitly blacklisted in the UCPD**. BEUC pointed to the fact that some Member States are already considering regulating or have already regulated influencers at national level as evidence of the need for stricter EU rules. They also suggested that liability should be extended. *"Influencer marketing is often a 'value chain' between influencers, influencer agencies, platforms, and brands. To tackle hidden advertising practices, the liabilities of each actor should be clarified during the Commission's fitness check process, with particular attention to rules on joint liability of influencers, agencies and brands in case of breach of transparency requirements."* The European Parliament's IMCO Committee has also done research into the impact of influencers on consumer protection.⁸⁴ The study confirmed that at **EU level**, no specific legislation focussing on

⁷⁸ [mfl-english.pdf \(kfst.dk\)](#)

⁷⁹ Eight influencers reported to the Danish Consumer Ombudsman.
<https://www.lexology.com/library/detail.aspx?g=1f65c488-b45d-4c14-b74e-3edb1d6cc5a5>

⁸⁰ <https://www.reclamecode.nl/nrc/advertising-code-for-social-media-influencer-marketing-rsm-2019/?lang=en>

⁸¹ <https://business.gov.nl/regulation/advertising-rules-social-media-influencers/>

⁸² www.asa.org.uk/news/updated-guidance-for-influencer-marketing.html#:~:text=Consumers%20must%20always%20be%20aware,of%20action%20from%20the%20ASA.

⁸³ https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/influencer-legal-hub_en

⁸⁴ The impact of influencers on advertising and consumer protection in the Single Market, Study for the EP's IMCO Committee - [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703350/IPOL_STU\(2022\)703350_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703350/IPOL_STU(2022)703350_EN.pdf)

influencer marketing is in place. However, there are several pieces of EU legislation to take into account when analysing the regulation of influencers that address influencer marketing horizontally. The study notes that "certain rules apply more to influencer marketing as an advertising activity, while others cover influencers who act as sellers." The study noted that "the fast-growing market of influencers comes with potential risks for consumers and creates several challenges for regulators". The lack of adequate disclosures by influencers breaches existing EU consumer protection rules, for instance in relation to hidden advertising in the UCPD. This raises a question as to whether existing EU rules are sufficient to ensure adequate transparency by influencers regarding the commercial nature of content.

BEUC advocated⁸⁵ making several changes to the existing EU legal framework, such as providing a definition of "influencer marketing" in the UCPD and clarifying that any publication from a content creator against any kind of paid consideration, should be sufficient to qualify as a commercial intent and be subject to disclosure requirements. However, unlike other national legal frameworks e.g. in FR and NL, rather than setting a minimum threshold for what constitutes a professional or major influencer, they suggest that the *"size of the influencer audience, the recurrence with which they run commercial partnerships with brands and the fact that brands have control or not on the content of the publication should be irrelevant."* They also advocate amending the UCPD Annex (Points 11 and 28 of the blacklist) to introduce "user-generated content" as a concept. This notion is broader in scope than the current wording "editorial content". In BEUC's view, this would *"bring legal clarity and ensure that all contents posted by content creators are subject to the transparency rules, irrelevant if users promoting products on a sparse or recurrent basis."*

Opinions among wider stakeholders were mixed regarding **whether influencers need to be categorised as a specific type of trader**. Whilst some Ministries and consumer Ombudsmen supported this as a means of clarifying that influencers fall within the existing scope of EU consumer law, others argued that they are (implicitly) covered in the definition of a trader. The main applicable rules e.g. hidden advertising has been prohibited on a longstanding basis and the guidance can provide examples as to the latest practices that are prohibited such as influencers disguising their views as being impartial when they are being paid.

The **Finnish competition and consumer authority** noted that influencer marketing is not fundamentally different from marketing practices employed by traditional marketing channels, for which a large body of legislation already exists. The UCPD can already be applied to influencers so long as they qualify as traders, though as noted earlier, the challenge is the current lack of a clear definition in this regard. **Seldia, the European Direct Selling Association**, also expressed the view that the UCPD is already adequate to address the challenges. Many industry stakeholders attributed the problem to weak enforcement, and jurisdictional challenges in enforcing cases involving non-compliance with EU law outside the EU. Overall, drawing on our analysis of the case study and desk research concerning social commerce and influencer marketing, it can be concluded that:

- Influencer marketing is already partially addressed in EU consumer protection law and in other relevant laws, but in the case of consumer law, only indirectly. There is an absence of a clear set of rules integrated into a single legal framework.
- There is a need for a clear definition of an influencer in EU consumer law to avoid a situation whereby non-professional influencers avoid their legal obligation to inform consumers there is commercial intent underlying influencer marketing communications.
- The absence of clear rules for influencers with respect to social commerce and

⁸⁵ BEUC, 2023. FROM INFLUENCE TO RESPONSIBILITY - Time to regulate influencer marketing, BEUC position paper, July 2023 - [BEUC-X-2023-093 From influence to responsibility Time to regulate influencer-marketing.pdf](#)

marketing practices by influencers undermines the effectiveness and enforcement of EU consumer rules, especially given evidence that there are higher levels of non-compliance with existing rules among influencers compared with other types of traders.

2.1.8 Digital addiction

This section considers issues around digital addiction generally, but also considers a few specific issues where problems have been identified by some stakeholders and in some research, such as loot boxes and virtual items.

2.1.8.1 Digital addiction – nature of problem and key drivers

RQ10 – What are the drivers of digital addiction and what are the challenges for legislators in addressing this problem area?

Digital addiction is a broad concept, which may cover a range of addictions that consumers may have with respect to digital goods and services. There is the general problem of internet addiction and addiction to digital devices more generally, which may lead to adverse mental health consequences of excessive screen time. Examples are: people addicted to social media, certain types of online gaming, and the use of paid loot boxes, which can be more addictive for minors. The problem of digital addiction among video game players is mentioned in the UCPD guidance, in particular techniques to maximise the amount of time people play the game and means of increasing in-game spending.

Digital addiction, or internet addiction is not currently listed in relevant collections among substance-related disorders (e.g., smoking, alcohol) **and behavioural disorders** (e.g., pathological gambling), and not included as a diagnosis 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). However, in 2013, **internet gaming addiction was entered into the DSM-V as the first digital addiction disorder**. Other disorders triggered by digital products⁸⁶ are still only in the appendix of the DSM-V and under discussion, due to a lack of pathological evidence and research required to reach consensus that they should be entered into these collections.

There are also discussions ongoing among researchers whether extensive use of digital products is an addictive tendency or merely a **rapid adoption to new social norms** (e.g., in the context of smartphones). Some researchers also find that since the symptoms of digital addiction have a strong overlap with tendencies toward depression and attention deficit hyperactivity disorder, digital addiction may just be a **mere symptom of other disorders**.⁸⁷

However, research has also identified the extent to which disorders triggered by digital products **share certain symptoms with other behavioural addictions** (e.g., antisocial and risky use, altered value-based decision-making) and Kuss et al. (2014)⁸⁸ introduced an **internet addiction model** that summarises all symptoms used to diagnose internet addictions, namely **salience, mood modification, tolerance, withdrawal, relapse and conflict** – all of which resemble strongly symptoms observed in other substance and behavioural addictive disorders. Similar to substance-related addictions and behavioural disorders is also the observation that disorders triggered by digital products do not only manifest via technology, gadgets and services, but the **person's context and personality, specific situation, resilience and coping strategies** all influence the development of

⁸⁶ Examples are social media addiction, mobile phone addiction, addiction to loot boxes within video games.

⁸⁷ Leo K. et al. (2021) Depression and social anxiety predict internet use disorder symptoms in children and adolescents at 12-month follow-up: results from a longitudinal study. *Front. Psychol.* Link: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8710475/>

⁸⁸ Kuss D. J. et al. (2014) Internet addiction: a systematic review of epidemiological research for the last decade. *Curr Pharm Des.* Link: <https://pubmed.ncbi.nlm.nih.gov/24001297/>

addiction.⁸⁹ As in other types of addictions, individuals become more prone to digital addiction due to reasons such as easy access, limited self-control and increased peer pressure.⁹⁰ In addition to these factors, exposure to technology can be considered another important antecedent.

In terms of drivers of addictive behaviours in the context of digital products, research⁹¹ has identified the following as **mechanisms that can exploit users' psychological vulnerabilities to maximise time spent and daily visits**, which can lead to problematic behaviour:

- **Recommender systems** make personalised recommendations to users of any online application; they may be ads, trending content, posts, friends (“friends you may know” feature on social media) or comments. The main segment of any recommender system is an algorithm, which may be a set of simple straightforward rules dictating how the content is being processed, or it can use artificial intelligence. The main purpose of recommender systems is to keep users engaged by presenting personalised content to them by harvesting their data, analysing it, and delivering content based on the outputs of this analysis. While undoubtedly this is a mechanism that can improve the overall user experience with a service that is designed to maximise utility, they can become an instrument to “trap” the user into the system; this is especially the case, if there are misalignments between the goals of the service or app and the user’s utility in terms of digital wellbeing, and recommendations are delivered endlessly during and outside of the user’s interaction with the service or app.
- **Autoplay** – a mechanism where new contents like videos or stories are sequentially and automatically played without the need for a user’s interaction, meaning it removes the need for autonomous decision-making; research found that autoplay often makes users feel less in control by undermining their sense of agency, as suggestions of new videos are “hard to decline.”
- **Pull-to-refresh** – a mechanism allowing users to “pull” an interface, e.g., by swiping down on a mobile app, to manually reload the status of the system for new content; researchers have found that this mechanism offers a variable reward to users in that it may or may not reveal new content, meaning that it exploits the same psychological vulnerabilities that are targeted in gambling addictions.
- **Infinite scrolling** – a mechanism through which new content emerges automatically and continuously as users scroll down a page, which researchers have also related to the concept of variable reward, since it creates the illusion that new interesting contents will “flow” forever, while the “quality” of the next shown item cannot be predicted.
- **Social investment** – metrics like number of reactions, comments, followers and views can make users “invested” in a platform; this mechanism can instil in users the idea that they should continue using the platform to avoid losing the achieved progress; researchers also found that social networks are sometimes designed to structure rewards in a way that is likely to encourage use (e.g., notifications on Facebook about a “like” can be delayed to maximise its reward).
- **Non-Fungible Tokens (NFTs)** – NFTs represent digital assets verified and stored using blockchain technology. Each NFT carries a unique signature that makes it

⁸⁹ Brand M. et al. (2016) Integrating psychological and neurobiological considerations regarding the development and maintenance of specific internet-use disorders: an interaction of person-affect-cognition-execution model. *Neurosci Biobehav Rev.* Link: <https://pubmed.ncbi.nlm.nih.gov/27590829/>

⁹⁰ Griffiths, M. and Wood, R (2000). Risk factors in adolescence: the case of gambling, video game playing and the internet. *Journal of Gambling Studies*, 16, 199-225.

⁹¹ Roffarello, A. and Russis, L. (2022) Towards understanding the dark patterns that steal out attention. CHI EA '22: Extended abstracts of the 2022 CHI conference on human factors in computing systems, Article 274.

difficult to replicate, which is why NFTs cannot be traded or exchanged at an equivalent price. They can be used to purchase digital items, such as objects in video games, pieces of art, or music. There have been attempts by Meta to launch a cryptocurrency payment system in the past, which were halted by US regulators. However, future tokens might be earned by engaging in social media platform's activities, such as posting, commenting, providing reviews or linking/disliking content. NFTs have been likened to gambling in that participating in NFT transactions is characterised by taking risky actions with the hope that the result will be beneficial. Purchasing NFTs can thus trigger the brain's reward system, and if these behaviours are not regulated, result in financial problems for the consumers, separate them from their loved ones, and lead to depression or anxiety.

- **In-app or in-game purchases** can take many forms, like a virtual currency that enables to buy faster progress in the game, power-ups to improve gameplay, items to personalise the player's avatar, and premium content that grants access to exclusive features or levels. They usually require small amounts of real money to access virtual items or currency within the game. The basic design and implementation of in-game purchasing options, particularly their rapid pace, repeatability, and inherent randomness in some formats (e.g., loot boxes), has invited some comparisons to gambling products, particularly electronic gaming machines.⁹² We discuss these further when addressing loot boxes.
- **Gamification** means the integration of game-like elements into non-gaming environments, such as training apps or mobile games in online casinos. The technology encourages users to compete against each other, collect points and increase levels. Gamers are rewarded for their achievements, and, at the same time, encouraged to continue to develop constantly. Gamification works as a strategy to influence and motivate people's behaviour. However, according to literature, some game features and sensations like flow can be regarded as addictive factors, triggering **a dopamine rush in the human brain** – hence they are often harnessed by websites and apps to retain their users, who come back for more dopamine release.

Digital addiction is similar to the consequences of other types of addictions. These include sleep problems, psychiatric problems, loneliness, anxiety, stress and depression⁹³. In addition, neglecting social life and family can be considered among social problems. Das et al. (2017)⁹⁴ state that almost 80% of online gamers have lost at least one element of their lives such as sleep, work, education, or socialising with friends or family.

In terms of **social media addiction**, Moqbel and Kock (2018) found that addiction to social networking sites reduces positive emotions which increase performance and improve health, resulting in an increase in attention deficit.⁹⁵ Zheng and Lee (2016)⁹⁶ also show that social media addiction leads to three types of conflicts: tech-personal, tech-family and tech-work. In their recent report, the 5Rights Foundation also notes that **children and young people themselves increasingly describe their usage and engagement with digital services**

⁹² King D. and Delfabbro P. (2018) Internet Gaming Disorder: Theory, Assessment, Treatment and Prevention. Academic Press.

⁹³ Jorgenson, A. et al. (2016) Internet addiction and other behavioural addictions. Child Adolescent Psychiatry Clin N Am. Link: <https://pubmed.ncbi.nlm.nih.gov/27338971/>

⁹⁴ Das A. et al. (2017) Technology addiction and mental health. Indian Journal of Psychological Medicine, Vol. 39, Issue 1. Link: <https://journals.sagepub.com/doi/pdf/10.4103/0253-7176.198939>

⁹⁵ Moqbel M. and Kock N. (2018) Unveiling the dark side of social networking sites: personal and work-related consequences of social networking site addiction. Information and Management 55. Link: http://cits.tamtu.edu/kock/pubs/journals/2018/Moqbel_Kock_2018_IM_DarkSideSocNtwk.pdf

⁹⁶ Zheng, X. and Lee, M. (2016) Excessive use of mobile social networking sites: negative consequences on individuals. Computers in Human Behaviour, Vol. 65. Link: <https://www.sciencedirect.com/science/article/abs/pii/S0747563216305751>

using language associated with addiction. A 2022 survey by YoungMinds⁹⁷ found that 42% of young people self-reported early signs of addiction to social media.⁹⁸

The EP's IMCO Committee in July 2023 put forward an EP-own initiative on digital addiction, which was adopted as a resolution in the EP Plenary in December 2023. It notes that:

“Many digital services, such as online games, social media, streaming services for films, series or music, online marketplaces or web shops and dating apps are designed to keep users on the platform for as long as possible so as to maximise the time and money they spend there; whereas consequently many online services are designed to be as addictive as possible; whereas the terms ‘addictive design’ or ‘behavioural design’ of online services describe features that lead to behaviour-related forms of digital addiction, such as, ‘excessive or harmful internet use’, ‘smartphone addiction’, ‘technological or internet addiction’, ‘social media addiction’; whereas there is a growing consensus among academics that phenomena, such as ‘social media addiction’ exist”;

In addition, the EP report notes the problem that digital addiction is concentrated but not confined to young people, including minors and young adults.

“Whereas 16-24 year-olds spend an average of over seven hours a day on the internet; whereas one in four children and young people display ‘problematic’ or ‘dysfunctional’ smartphone use, meaning behavioural patterns mirroring addiction; whereas research suggests that problematic smartphone use continues to rise; whereas research also suggests that the rise in mental health problems in adolescents might be related to excessive social media use”

The report also points to a number of harmful consequences of different forms of digital addiction.

“Whereas internet-use-related addiction displays similar side effects to substance-related addictions, including evidence of tolerance and relapse; whereas strict regulation exists for addictive products, such as drugs, alcohol, tobacco and gambling to prevent addiction and protect consumers from harm; whereas problematic smartphone or internet use has been linked to lower life satisfaction and mental health symptoms such as depression, low self-esteem, body-image disorders, eating disorders, anxiety, high levels of perceived stress, neglect of family and friends, loss of self-control, lack of sleep and obsessive-compulsive symptoms, such as compulsive buying among young adults; whereas heavy users of digital media are twice as likely to have mental-health issues, including risk factors for suicide and self-harm; whereas children and young people are more vulnerable to these symptoms; whereas mental-health conditions established in childhood can shape an individual’s subsequent life course; whereas excessive internet use is associated with problems with daily obligations, declining grades, poor school and academic performance or poor job performance”

A challenge in addressing the problem of digital addiction is that whereas some areas may be regulated e.g. online gambling, many issues have societal and health-related consequences, but are not presently explicitly regulated in EU consumer law, although there is general protection for children and for vulnerable consumers on the grounds of age (what the latter means is not specified in Art. 5(2) of the UCPD). Moreover, in our case study, we identified three “components” of digital addiction development (situation management, access

⁹⁷ [A third of young people feel trapped on social media | YoungMinds](#)

⁹⁸ [5Rights Foundation Disrupted Childhood 2023](#)

management / decision support / gratification management), highlighting under each the areas where legislation can potentially “step in” to prevent and/or limit the potential negative effects on the social and financial situation of consumers due to addiction and prolonged use of certain digital content and services. These concern, in particular:

- the “deployment” of addictive features in digital products (situation management), namely guidance, regulations and/or bans of specific design features which are known to pose a risk for digital addiction development in general, or with reference to specific consumer groups (e.g., vulnerable consumers and/or minors),
- information provision about addictive design features (access management / decision support), meaning legislation that may inform issues of transparency, completeness, and what is defined as a problematic “default” setting,
- mechanisms that can potentially break the instant and limitless gratification provided through digital tools (gratification management) and thus curb digital addiction development, such as legislation concerning parental controls and time and cost limitations.

In our case study, we assess the extent to which existing consumer law Directives, other and relevant EU and national legislation adequately address digital addiction development, and whether there is scope to include specific rules in the Directives. In some areas of the digital economy, such as social media platforms, and hardware producers of digital devices, interview feedback noted a range of tools that have been developed to help consumers (including the parents of minors) to monitor and limit screen time at the device or console level and/ or in-app. Features such as time out and screen time daily and weekly monitoring tools can be used on smart phones and tablets and set within certain platforms. Whilst trader associations and tech firms including platforms interviewed recognised the seriousness of the problem, they highlighted the existing measures they already take to tackle the problem.

2.1.8.2 Loot boxes and virtual items

Loot boxes are a type of in-app purchase, usually present within video games, that contain uncertainty-based rewards (e.g. opening a mystery box to obtain other virtual items).

Regarding annual spending on loot boxes per consumer:

- In 2019, the average lifetime spending on loot boxes in the US was 217 USD per player (200 EUR).⁹⁹
- 40% of adult gamers 21 and older have purchased loot boxes (Brooks & Clark, 2019) and 44% of adults have spent money on loot boxes.¹⁰⁰
- According to an annual survey by IPSOS undertaken for Video Games Europe, just 9% claim to have spent real money on in-game currency and less than 4% on loot boxes.¹⁰¹ The study found that in selected EU countries, the majority of children (64%) spends between €1-20 average / month. On average, spend has increased by €6 per month amongst those who claim to spend, vs. 2020, in line with inflation.
- There appears to be a downward trend in that whereas 42% of children playing video games were spending money on in-app purchases, this had declined to 18% by 2023.

⁹⁹ The U.S. console gamer average lifetime loot box spend 2019 - published by J. Clement, Aug 25, 2023.

¹⁰⁰ Loot box consumption by adolescents pre- and post- pandemic lockdown Whitney DeCamp and Kevin Daly. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10158757/>

¹⁰¹ https://www.videogameseurope.eu/wp-content/uploads/2023/09/Video-Games-Europe_In-Game-Spending-2023_Final-Sept.pdf

In terms of how much time the average consumer spends on loot boxes, Video Games Europe, the EU association for the gaming industries, has made data available previously.¹⁰² Data on the extent of usage of video games is provided below. On average, people in Europe spend:

- 9 hours/week playing video games, 14 hours/week on social media, 24 hours/week on watching TV.
- 53% of the population between the ages of 6 and 64 plays video games.
- Player base increased by 1.4% between 2021 and 2022
- 32 is the average age of a video game player in Europe. 18% 6-14 years old, 21% 15-24 years old, 19% 24-34 years old, 17% 35-44 years old, 25% 45-64 years old.
- 46.7% of European game players are women, 33 is the average age of women who play video games, 44% of women video game players are 35-64 years old, women represent 51% of all smartphone and tablet players.

Among the main concerns from a consumer protection perspective from loot boxes are:

- Loot boxes have been linked in research by consumer associations to a wide variety of problematic practices, such as **deceptive design, aggressive marketing, and misleading probabilities regarding randomisation odds**.¹⁰³
- The risk that video game loot boxes may be linked to **problem gambling**, even if literature varies in terms of conclusively establishing a causal link.¹⁰⁴
- The risk that loot boxes may lead to **digital addiction**, especially in online-gaming, with the potential to exploit young consumers.
- The lack of any EU consumer law rules on loot boxes. Loot boxes are currently neither prohibited or regulated, which it could be argued has led to the emergence of national rules on loot boxes in some countries. A risk of regulatory fragmentation and undermining of the single market due to the lack of uniform rules on loot boxes at EU level, given the pan-European and global nature of the games industry. The absence of uniform rules on lootboxes in third countries has also been recognised internationally.¹⁰⁵
- Moreover, there are differences in regulatory approaches as to whether loot boxes constitute gambling or not at national level. In most MS (e.g. in Denmark, Finland, France, Sweden, Germany, Poland), loot boxes are not considered to be gambling, whereas in other countries, such as **Belgium, the Netherlands and Slovakia**, loot boxes are considered (or were considered by some regulators) to be gambling. Even in these countries, there have been debates as to whether loot boxes constitute gambling or not, and about whether they should be prohibited altogether or should be regulated and how.
- The absence of rules on transparency regarding the randomisation odds when

¹⁰² Video Games Europe: https://www.videogameseurope.eu/wp-content/uploads/2023/08/Video-Games-Europe-Key-Facts-2022_FINAL.pdf

¹⁰³ Report "INSERT COIN: How the gaming industry exploits consumers using loot boxes" (2022), Norwegian Consumer Council (NCC) - <https://storage02.forbrukerradet.no/media/2022/05/2022-05-31-insert-coin-publish.pdf>

¹⁰⁴ Zendle D, Cairns P (2018) Video game loot boxes are linked to problem gambling: Results of a large-scale survey. PLoS ONE 13(11): e0206767 10.1371/journal.pone.0206767

¹⁰⁵ Derrington, Stephanie & Star, Shaun & Kelly, Sarah. (2021). The Case for Uniform Loot Box Regulation: A New Classification Typology and Reform Agenda. Journal of Gambling Issues. 46. 302. 10.4309/jgi.2021.46.15.

consumers purchase virtual items, such as those contained in loot boxes.

The problem of loot boxes and other addiction-inducing design features was attested to in the targeted survey. The results show that 75.7% of respondents either agreed or strongly agreed that these features are problematic. However, 8.6% disagreed and 15.7% disagreed strongly.

Table 2-5 – To what extent do you agree or disagree that the following practices are problematic? Use of loot boxes and addiction-inducing design features (in digital services such as video games).

Response options	Number	%
Strongly agree	31	44.3%
Agree	22	31.4%
Disagree	6	8.6%
Strongly disagree	11	15.7%
Grand Total	70	100%

Source: targeted survey

In some countries, national legislation on loot boxes has emerged, which risks undermining an EU harmonised framework to address any unfair commercial practices in this domain. A number of Member States have been reflecting on how best to regulate loot boxes, or given EU competence on unfair practices, whether to legislate at all.

Regarding interview and position paper feedback, some stakeholders, such as consumer associations and some national CPAs, would like loot boxes either to be banned, or at least to be regulated. Some stakeholder consider loot boxes to be “blurring the lines” between gaming and gambling for consumers. Consequently, loot box purchases may be linked to a variety of harms, including accentuating the problem of online gambling.¹⁰⁶ Whilst loot boxes and other randomised event features have not been shown to have a direct causal relationship with problem gambling among general users in the first instance, there nonetheless remains, a critical unanswered question for legislators around how to, as a minimum, protect vulnerable consumers against such proxy or veiled gambling; with a particular consideration for the way in which the design and advertisement of such in-game products have often targeted children.

The rationale cited among stakeholders that want to prohibit or restrict loot boxes is that they may constitute, or promote gambling, especially among young people who are more vulnerable and prone to digital addiction. The issue of loot boxes and how far this raises consumer protection issues is considered in detail in the case study on digital addiction.

A study by the **Norwegian Consumer Council (NCC)**, supported by 20 different consumer associations provided evidence on how and why loot boxes contribute to digital addiction¹⁰⁷. The NCC’s report outlines several ways in which loot boxes exploit consumers, such as deceptive design, opaque algorithms and skewed probabilities, aggressive marketing, in-game currencies, and hidden pricing.

Other respondents to the public consultation such as Ministries and consumer ombudsmen expressed concerns about the need to protect minors in that loot boxes are a potential conduit to encouraging children and teenagers into engaging in other forms of gambling once they get older. The issue of protecting minors was raised, for instance, in public consultation position

¹⁰⁶ [Government response to the call for evidence on loot boxes in video games - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/consultations/evidence-on-loot-boxes-in-video-games)

¹⁰⁷ INSERT COIN - How the gaming industry exploits consumers using loot boxes 31.05.2022, <https://storage.forbrukerradet.no/media/2022/05/2022-05-31-insert-coin-publish.pdf>

papers received from BEUC and the Danish Ministries responsible. This is also reflected in key literature¹⁰⁸.

The **Dutch Consumer and Markets Authority (ACM)** asked the Commission to consider *“Demand[ing] from businesses that, when presenting prices that are displayed in in-game or in-app currency, those prices are also presented in real money – and to consider further action than just transparency requirements and legal regime, but prohibiting loot boxes, specifically in relation to children.”* ACM propose that the Commission considers giving consumers the “same or similar rights when in-game and in-app purchases are made with in-game or in-app currencies as for in-game or in-app purchases with real money”. For example, it could be stipulated in the Unfair Contract Terms Directive (or in a blacklist of prohibited practices) that **in-game and in-app currencies that do not provide a real-world equivalent to ensure transparency for consumers as to the real cost would be non-refundable as an unfair contract term.**

Stakeholder views on whether loot boxes should be permitted, prohibited, or regulated are now considered. **BEUC** advocated in their public consultation position paper that measures should be taken at an EU level to tackle the problem of loot boxes. Their recommendations were as follows:

- 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**;
- An obligation should be introduced to disable in-game payments and loot boxes mechanisms by default;
- Solutions are needed for **more transparency**: researchers and regulators should have access to the algorithms and datasets that are involved in the loot boxes to conduct independent research in the public interest;
- Consumers should have the option to use the game **without algorithmically driven decision-making** that aims to influence consumer behaviour;

They also suggested that if other remedies do not alleviate the problems, a full ban of ‘paid’ loot boxes should be considered.

The **European Game Developers Federation (EGDF) and Video Games Europe (VGE)**, representing the trader perspective, were not in favour of introducing new requirements into EU consumer law on loot boxes. They stated in public consultation position papers that they supported voluntary initiatives by industry to address the problem of loot boxes (in the same way that the UKIE has developed a joint initiative between UK Government and industry to achieve common policy objectives by setting out a set of industry-agreed principles to protect consumers. They produced industry-led guidance in the form of 11 principles “designed to meet UK Government objectives to improve protections for players.”¹⁰⁹ Examples of some of the principles are: Make available technological controls to effectively restrict anyone under the age of 18 from acquiring a loot box, without the consent or knowledge of a parent, carer or guardian and drive awareness of, and uptake of technological controls with players, parents, carers and guardians through regular communications, starting with a targeted public information campaign.

The EGDF pointed to several voluntary industry-led measures to ensure parental controls in games consoles and software and apps to ensure that minors cannot spend money on loot

¹⁰⁸ A Cerulli-Harms, M Münsch, C Thorun, F Michaelsen and P Hausemer, Loot boxes in online games and their effect on consumers, in particular young consumers, 2020, 24, available at <https://op.europa.eu/en/publication-detail/-/publication/56bb7432-cc8a-11ea-adf7-01aa75ed71a1/language-en/format-PDF>

¹⁰⁹ 11 principles “designed to meet UK Government objectives to improve protections for players <https://ukie.org.uk/loot-boxes>

boxes without an adult's permission. Among the examples of the schemes mentioned to tackle the problem are:

- A voluntary commitment among video game publishers to **strengthen disclosures of the probability of obtaining randomised virtual items in paid loot boxes**. The disclosure commitment applies to all new games and any updates made to existing games that subsequently add this type of in-game purchase. The disclosures are meant to be made in a manner that is understandable and easily accessed. It was also noted that since 1 October 2020, major console makers (e.g. Microsoft Xbox, Nintendo, and Sony PlayStation) – have required publishers to disclose probabilities of paid random items (loot boxes, card packs) in new games and game updates.
- The disclosure rules are designed to **improve transparency for consumers regarding purchasable random content, such as loot boxes**, to ensure that **the chances of winning are made clear to game users during in-app play**. The practice of transparency through disclosures about the odds of winning was subsequently incorporated into the UCPD guidance document, and this was welcomed by trader representatives.
- A longstanding commitment by **major console manufacturers (e.g. Microsoft Xbox, Nintendo, and Sony PlayStation) to strengthen parental controls at the point of setting up of games controllers**.

The EGDF and VGE noted that the Commission's UCPD Guidance provides an interpretation of the existing law that disclosure requirements should be made to inform consumers and players before purchasing a game if it includes paid random elements. The guidance also states that traders should make use of parental controls at the platform level to disable spending, which the trader association describes as being "important instruments to mitigate any unwanted spending, as well as manage playtime and online interactions". Data on the prevalence of in-game spending in a 2023 study for VGE on In-Game Purchases in European Markets¹¹⁰ suggests that loot boxes remain a relatively small and static feature in the digital products landscape. The study examined also the extent to which minors are spending on loot boxes, finding the following:

The proportion of parents claiming their children don't spend on in-game extras remain stable. More than 3 in 4 parents **(76%) claim their children don't spend on in-game extras** within the video games they play. The majority of children (64%) spend between €1 - €20/month on average. This has increased by €6 per month amongst those who claim to spend, versus in 2020, in line with inflation. The most popular in-game extras categories are content that either impact gameplay or are decorative or cosmetic. The most popular content is the one that impacts gameplay (34%), with **just under one third spending on in-game extras on decorative or cosmetic items** (which do not impact gameplay). Unknown rewards, such as **Loot Boxes, are less popular**.

The number of parents of children who spent on in-game extras and have an agreement on spend levels remains high. 9 in 10 parents of children who spend on in-game extras have an agreement with their children about spending limits. Half (506) have an explicit agreement with their children, either asking permissions (38%) or setting spending limits (23%). Most video game players don't engage with, or are not aware of in-game currency purchasing nor loot boxes. Just 9% claim to have spent real money on in-game currency and less than 4% on loot boxes.

Source: IPSOS for Video Games Europe, 2023.

Academic stakeholders and position paper submissions during the present study from EGDF along with the Dutch Consumer and Markets Authority and Française des Jeux (FDJ) lottery

¹¹⁰ In-Game Purchases in European Markets (2023) - IPSOS for Video Games Europe. <https://www.videogameseurope.eu/publication/in-game-purchases-in-european-markets/>

operator recognised the **blurring of lines between gaming and gambling** as a development in relation to in-game purchases of virtual goods. Games of chance more often now form a key social or gameplay component of the overall game experience. Academic research on the small number of high-spending digital product consumers has concluded that “games developers (unwittingly or not) are disproportionately profiting from moderate and high-risk gamblers, rather than high earning customers. Such patterns of spending mirror those observed with gambling revenues, and have implications for harm minimisation and ongoing policy debates around loot boxes.”¹¹¹

National regulatory frameworks on loot boxes

There have been some developments in national law towards regulating loot boxes though presently, several initiatives remain at the regulatory proposal stage.

- The only jurisdiction where loot boxes are currently restricted is **Belgium**, where the Gambling Commission declared loot boxes to be in violation with gambling legislation in 2018 when they fall under the definition of ‘games of chance’. However, a regulatory review of the position on loot boxes is currently underway. According to the VGE, there are concerns whether a blanket ban on loot boxes has worked. A recent study showed that the Belgian regulator is experiencing difficulties in enforcing the ban, given the global nature of the games industry¹¹² and that major platforms through which free video games are downloaded are global rather than national. However, in most MS (e.g. in Denmark, Finland, France, Sweden, Germany, Poland), loot boxes are not considered to be gambling.
- A **draft bill in Spain** proposes to **prohibit access to loot boxes for minors**, meaning that anyone under the age of 18 will be prohibited from accessing loot boxes, and companies will have to verify user IDs before they can access a loot box, which may include biometric identification systems.
- Currently, **Dutch law** does not specifically regulate video games or loot boxes, but it does regulate some areas of gaming which may appear in video games and in respect of the provision of games of chance. The Netherlands is however considering legislation on loot boxes in future. 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’. Several jurisdictions do not consider features like loot boxes as gambling because of the impossibility of ‘cashing out’ in real currency.

Whilst some stakeholders (e.g. Ministries, CPAs) favoured regulating loot boxes, there were divergent views as to how best to regulate in this area. For instance, the Netherlands Authority for Consumers and Markets (ACM) was in favour of regulating loot boxes, along with some Scandinavian CPAs. ACM raised various concerns relating to loot boxes in their public consultation response that stemmed partially from the absence of clear EU rules on loot boxes.

“Loot boxes contain features that strongly resemble gambling practices, thus substantiating a substantial risk for gambling addiction among consumers. A consumer will not know in advance what rewards the loot box will offer, while more and less valuable rewards are not evenly distributed in terms of winning probabilities. Despite the gambling-related features, it is not clear if and to what extent loot boxes are covered by gambling law”.

The ACM suggested ways of improving the lack of legal certainty to ensure higher levels of consumer protection (especially for minors). They recommended that there should be a

¹¹¹ Close, J. et al. (2021) ‘Secondary analysis of loot box data: Are high-spending “whales” wealthy gamers or problem gamblers?’, *Addictive Behaviors*, 117, 106851.

¹¹² Xiao, L.Y. (2022) ‘Breaking Ban: Assessing the effectiveness of Belgium’s gambling law regulation of loot boxes’. Available at: <https://doi.org/10.17605/OSF.IO/5MXP6>.

prohibition of loot boxes for children and that there was a need to clarify the legal regime for users of loot boxes beyond minors, for instance by regulating on issues such as ensuring transparency in winning probabilities in randomised prizes, marketing practices etc.”

However, there were concerns among some stakeholders that an outright ban on loot boxes would be competitively damaging for the European games industry, and questions as to the proportionality of such a step. The European Games Developer Federation (EGDF) representing 23 national trade associations stressed the importance of voluntary initiatives by industry to tackle problems around loot boxes. In August 2019, the industry announced a voluntary commitment to provide improved transparency for consumers regarding purchasable random content, such as “loot boxes”. This consisted of two parts: one by console makers – Microsoft Xbox, Nintendo, and Sony PlayStation – and a commitment by video game publishers. *“The commitment requires the disclosure of the relative rarity or probability of obtaining randomised virtual items in paid loot boxes.”*

In the ELI public consultation position paper, it was argued that there was a need to regulate the problem at its core rather than to ban loot boxes altogether. *“At least concerning minors – [the main problem] is the limited availability and use of (parental) controls. If parents used more parental control options, there would be less need to protect minors against in-game loot boxes and the like.”*

2.1.8.3 The impact of digitalisation on people’s mental health

Increasing digitalisation has led to problems around digital addiction. The impacts are multi-faceted. For instance, this has had a negative impact on the people’s mental health, especially among children and young people. The Commission adopted a Communication on a comprehensive approach to mental health¹¹³ in June 2023. It identifies 20 flagship initiatives and EUR 1.23 billion of opportunities for financial support from several EU funding instruments.

The Communication focuses particularly on supporting vulnerable groups, such as children and young people. They are particularly vulnerable and we need to protect them during their most vulnerable and formative years. They face challenges due to over-use of digital tools – including use of social media – which puts increasing pressure on their mental health. Whilst recognising that many young people enjoy social media, there are several associated challenges, partly from digital addiction, but extending beyond this to a range of other issues. There is a need to ensure prudent use of social media to address issues such as online child grooming and sexual abuse, cyberbullying, hate speech, excessive screentime and the digital editing of images. A move towards a safer and healthier digital space for children and young people is needed. Some social media companies have taken action to address some of these issues, for instance, there are tools for users to monitor their own screentime, parental controls, buttons to alert content moderators to hate speech etc.

It should be mentioned that whereas some of these challenges potentially fall under the remit of consumer policy issues, e.g. excessive screentime, other problems and challenges may fall under other EU policies and laws. For example, content moderation responsibilities for platforms includes an obligation to remove hate speech under the DSA. There may be some issues which are inter-related between digital and consumer laws e.g. improving algorithmic transparency could help to avoid a situation in which content is pushed that is harmful to young people (e.g. self-harming content on social media platforms).¹¹⁴ It can be noted that some platforms have self-regulated through voluntary measures on this issue, though these were driven by regulatory pressures linked to previous tragedies.¹¹⁵

¹¹³ https://health.ec.europa.eu/system/files/2023-06/com_2023_298_1_act_en.pdf

¹¹⁴ Picardo J, McKenzie SK, Collings S, Jenkin G. Suicide and self-harm content on Instagram: A systematic scoping review. PLoS One. 2020 Sep 2;15(9):e0238603. doi: 10.1371/journal.pone.0238603. PMID: 32877433; PMCID: PMC7467257.

¹¹⁵ <https://about.instagram.com/blog/announcements/supporting-and-protecting-vulnerable-people-on-instagram>

The Communication on mental health recognises that people's health is influenced by their life experiences and environments in which they live. Four flagship initiatives have been identified in a dedicated chapter on 'Boosting mental health of children and young people', such as a children/youth mental health network, a prevent toolkit for children and a youth first flagship. One of the actions aimed at the better protection for children in the digital sphere, online and on social media, which is under the lead of DG CNECT. The Safer Internet initiative to protect children by CNECT can also be mentioned.

Regulators globally are looking into various issues concerning digital addiction. For instance:

- The US has considered regulating in this area through the proposed **Social Media Addiction Reduction Technology Act (SMART Act)** from 2019¹¹⁶. This aimed to prohibit social media businesses from using "practices that exploit human psychology or brain physiology to substantially impede freedom of choice", and to require social media firms to take measures to "mitigate the risks of internet addiction and psychological exploitation, and for other purposes". However, the legislation was not adopted, although its consideration **raised the profile of the challenge of digital addiction among young people and may have had an impact on some of the voluntary self-regulatory measures proposed by large social media platforms;**
- The **UK** Government's 2023 Online Safety Bill combined with the self-regulatory principles committed to by UKIE, the trade body for the UK games and interactive entertainment industry **has helped to address digital** addiction and has tackled some of the problems associated with loot boxes.
- In **Asia**, countries such as China and South Korea have also taken steps to regulate loot boxes and to protect children by restricting how much money they can spend. These third country examples are considered in further detail in EQ13(2), which maps interesting examples of regulatory approaches in third countries.

Traders interviewed, especially large platforms and big tech have stressed that they have developed many tools to address the problem, such as time limits, screentime monitoring at a systems and app level and parental controls. They also argued that there are alternative means of addressing the problem, such as a pop-up warning for users after a certain period when engaged in endlessly scrolling. Traders such as major social media platforms and tech firms were keen to address problems identified by consumer associations and other stakeholders to strengthen consumer protection whilst avoiding prescriptive legislation that would affect their design interface and impose changes and limitations.

Feedback was also received in relation to infinite scrolling from a consumer law academic interviewed, who argued that the UCPD lacks any specific rules on infinite scrolling yet this form of web design for mobile apps and platforms may exacerbate digital addiction. For instance, somebody may intend to spend a few minutes having a break but then spend significant time on platforms repeatedly 24/7/365. The academic noted that whilst time limits are a useful tool, this does not address the problem of digital addiction sufficiently.

Moreover, whilst the assertions made by some national Ministries and consumer associations that consumers "pay with their attention, engagement, activity and behavioural data" and by "allowing the platform to sell advertising space to other traders", which implies keeping the consumer on their platforms for as long as possible, this is difficult to legislate against, as **individual consumers have freedom of action, even if is evidently desirable to avoid problems linked to digital addiction.** The tools mentioned above (time limits, parental controls, daily and weekly monitoring) are a partial solution, but it should be recognised that free services on platforms in exchange for data are globally very popular. Moreover, business

¹¹⁶ [Social-Media-Addiction-Reduction-Technology-Act.pdf \(senate.gov\)](#)

models in the internet era are data-driven. It would therefore be difficult to ban such practices completely to eliminate problems relating to digital addiction, which encompass specific practices, such as loot boxes, but which constitute a broad societal problem overall.

Therefore, the development of any potential new, or modification of existing EU legislation must be mindful of the need to strike the right balance between supporting innovation and the competitiveness of the European economy and protecting vulnerable consumers, especially minors. Both the case study and the assessment of interview and public consultation feedback found that many stakeholders are concerned about digital addiction and its impact on minors. The lack of an explicit definition of what 'age' means in the definition of a vulnerable consumer in the UCPD was also highlighted as making it more challenging to protect young people. The absence of an EU-wide definition on what constitutes a 'minor' is a further obstacle. This issue is explored in further detail under external coherence, where the treatment of minors and children in EU consumer law and wider EU legislation is considered.

2.1.9 Dropshipping

Dropshipping is a way in which traders sell products online through e-commerce platforms and marketplaces without keeping them in stock. When an order is received, the seller sends the request to the producer or supplier and only then is the order processed, which means that consumers face potentially longer lead times before the product arrives. This practice has become much more common in recent years, due to large firms offering fulfilment services to process and expedite orders without sellers having to handle the stock directly. However, this creates problems regarding the lack of transparency for consumers who might reasonably expect that sellers hold stock themselves, especially if they are not informed about the dropshipping element of the business model. In the consumer survey, 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.

Some stakeholders responding to the targeted consultation, such as the French Ministry of the Economy (specifically the DGCCRF, Directorate General for Competition Policy, Consumer Affairs and Fraud Control) stated that transparency and consumer information should be further strengthened in the case of contracts with distance sellers practising dropshipping. In **France**, the influencer law also included a provision on dropshipping, which obliged influencers to inform consumers about key information, including the identity of the actual supplier and to ensure the availability and legality of the products and that they are not counterfeit products.

However, industry stakeholders in the dropshipping industry which represent firms specialising in logistics and fulfilment were against the idea of regulating dropshipping. A drop-shipping marketplace platform provider asserts that the Commission should recognise that European business models are inherently different to "Anglo-Saxon or Asian" approaches, with a foundation of shared values such as responsible sales and high customer satisfaction. They argue that European traders should be assumed to be acting in good faith and wish to deliver an improved digital environment for consumers. However, from a regulatory perspective, the issues are not to do with questioning the validity of dropshipping as a business practice that works efficiently for some traders, but rather whether transparency is needed in terms of information that a particular trader adopts a dropshipping model, given that consumers could potentially be disappointed if there are significant delays in receiving products due to the trader not holding stock and having to order from a third party where there are additional lead times. However, in some instances, lead times can still be rapid even if an intermediary places the order with a third party.

In the targeted consultation, 56.9% of respondents supported further consideration of additional transparency requirements in the EU legal framework for those using a dropshipping business model (30.6% responded offering no support for such additional requirements).

When analysing the issue of the effectiveness of EU consumer law and its enforcement, a challenge raised by the Ministry of Economy in France (targeted consultation position paper) was that enforcement powers and the means of action available to Member State CPAs are limited regarding **professionals established in third countries**, such as content creators and influencers. This could cause difficulties in ensuring adequate enforcement levels due to the global nature of this industry, as influencers fall under different EU laws such as the UCPD, the AMVSD (audiovisual content creators) and the DSA. The traders and platforms on which they operate may be located in countries globally with many different regulatory jurisdictions limiting the ease with which enforcement action can be taken, although the platform and marketplaces in the market do have to comply with EU legislation as otherwise they would encounter fines and reputational damage.

Position paper views from trader associations were that the prospect of further regulation or restrictions on traders causes concern for their members. Examples of those raising concerns were the trader association, **DOT Europe**, who argue that dropshipping is a legitimate business practice that should not be subjected to onerous rules. They urged caution when considering the adoption of legislation as they noted that their members have seen attempts at Member State level to legislate to strengthen transparency (e.g., see French Draft Law on Influencers). However, if an obligation for drop shippers to reveal the identity of their suppliers were to be introduced, this was considered as being a sensitive topic for many sellers as it could lead to disclosures beneficial to the competition as sellers would gain information about where other sellers were obtaining their products from, which they do not wish to reveal to their competitors.

However, a more basic transparency requirement could be to identify whether a particular seller practices dropshipping as it would then be up to the consumer to decide to purchase from a trader that does not hold stock directly.

2.2 Summary - national legislation to address problematic practices

EQ2 – Given the full harmonisation nature of the UCPD, to what extent can Member States regulate the problematic practices identified? Does the emergence of national legislation undermine the single market?

The UCPD is a maximum harmonisation Directive. However, through the case study and wider research, some recent and proposed new pieces of legislation were identified at national level in areas such as influencer marketing, subscriptions aiming to address problematic practices through more detailed rules than are present in the UCPD, which covers many topics through its wide material scope and general clauses. In addition, some national legislation aiming to protect minors was identified, such as the age verification of minors using social media platforms.

The development of national legislation in some MS regulating unfair practices through more specific rules than those in EU legislation points to various implications, namely:

- Whether the existing scope of EU consumer law is adequate already, or needs to be updated with more specific rules concerning problematic practices;
- Whether if other MS beyond those that have already introduced national legislation introduce their own rules on the same practices, this could bring into question the effectiveness of a fully-functioning internal market that ensures digital fairness through

EU consumer law;

- Whether given the full harmonisation nature of the UCPD, this could undermine the level playing field for traders, as traders doing business in some MS face additional rules beyond harmonised EU consumer protection rules relating to unfair, misleading and/ or aggressive commercial practices.

The following is a summary of relevant EU level directives that address or relate to key potentially problematic practices, but where at least some MS have introduced further national legislation, despite the UCPD's maximum harmonisation character. The analysis makes references to some national rules, but reference should be made to Section 2.1 on problematic practices, where national rules are described in detail by theme (e.g. subscriptions, influencer marketing, loot boxes). Some of the case studies in Annex 5 also provide a detailed mapping of national legislation:

- **Influencer marketing** – in most MS, influencer marketing is regulated in a similar way to any other form of marketing. Hidden adverts have long been prohibited through the UCPD and transposed nationally. The UCPD can apply to influencers where the influencer is engaged in commercial activities (thus acting as a trader), in particular Art. 5-7 of the UCPD and the accompanying UCPD guidance document confirms that in these circumstances social media posts and content can be considered as a commercial practice which must adhere to UCPD rules. Additionally, the AVMSD offers additional coverage and some overlap with the UCPD for influencers that produce on-demand audiovisual media content. There are several illustrations of how different MS have begun legislating in this area (further details are provided in the influencer marketing section (Section 2.1.7):
 - **France's Influencer Law** (2023)¹¹⁷ defines a social media influencer and differentiates between those carrying out influencer marketing as traders and individuals for whom it is a hobby.
 - **Italy** - proposed amendment to the Italian consumer code with a new annex concerning rules for influencers to strengthen transparency about paid promotions and sponsorship.
 - **Netherlands** - Dutch Media Act updated (2022), defining major influencers as those above the 500,000-followers threshold and publishing at least 24 videos per year. They must comply with the same advertising rules as on TV and must register with the Dutch Media Authority.
 - **Denmark** - the Danish Marketing Practices Act was updated in 2021 with new rules in relation to influencers, including prohibition of harmful commercial practices directed at specific customers, and children and young people.¹¹⁸
- **Online subscriptions** – there are general protections in the UCPD against unfair, misleading and/ or aggressive practices in subscriptions. The problem of subscription traps remains prevalent, with many complaints by consumers that they have been charged for subscriptions they no longer wanted, or have been charged when a free trial ended without being adequately informed that the free trial would automatically convert into a paid subscription when it expired. Some regulators, such as in **Germany (the cancellation button)**, **France (cancellation button, automatic renewal reminders)** and in **Belgium** (guidelines to clarify the form and content of fixed-term service contracts containing tacit renewal clauses), have taken the view that dark

¹¹⁷ Law of June 9, 2023 aimed at regulating commercial influence and combating the excesses of influencers on social networks

¹¹⁸ [mfl-english.pdf \(kfst.dk\)](#)

patterns are prevalent in subscriptions leading consumers to become trapped. The perception was that enforcement was inadequate to address the problem. Section 2.1.5 on online subscriptions provides further details on national rules.

- **Loot boxes** – whereas most MS do not have specific legislation on loot boxes, the topic has gained traction in recent years and several national laws have been proposed or are being considered. Examples are Belgium, where loot boxes were prohibited under gambling legislation, Spain where a proposal was made to prohibit sale of loot boxes to minors and the Netherlands, where there have been ongoing debates in the Dutch Parliament regarding a possible ban on loot boxes, with no decision taken as yet (see details of national legislation in Section 2.1.8.2).

Beyond the above-mentioned examples, it is also important to observe that there is also an international trend towards more specific regulation (and proactive enforcement of existing rules) to tackle problematic practices in the digital environment. For example:

- **Influencer marketing** – some regulators are considering regulating influencer marketing to strengthen transparency and/or have issued guidance to promote improved practices. UK and US regulators have expressed concerns regarding the need to strengthen transparency in paid promotions, sponsorship and partnerships. The **U.S. Federal Trade Commission (FTC)** has laid out guidelines that necessitate the use of informative hashtags such as #ad or #sponsored to disclose paid partnerships, enabling consumers to make informed choices. In the **U.K., the Advertising Standards Authority (ASA)** asks influencers to be transparent about advertising content. The guidelines on disclosure depend however on the influencer's relationship with the brand and the level of control the brand exerts over the content.
- **Subscription traps** – the UK introduced legislation on online subscriptions in May 2023. In the US, the FTC has taken action on subscription traps and dark patterns in a well-publicised case concerning Amazon Prime.

Stakeholder feedback on national legislation concerning digital practices deemed problematic

Different stakeholders have expressed different views as to whether national legislation can be justified. In the public consultation position papers, consumer associations and national Ministries responding were broadly supportive of the idea of extending rules in specific areas of digital markets and services in cases where there remain problems with non-compliance by traders, such as the problem of subscription traps. However, they would prefer a harmonised approach to be taken in all MS at EU level rather than a piecemeal approach with individual MS regulating challenges, such as age verification checks recently introduced in French legislation.

Trader associations interviewed were concerned about the implications of national legislation emerging in areas that have traditionally been covered by the UCPD due to the single market obstacles that these developments imply. Over time, there was a concern that if further MS also regulate these practices at national level, a patchwork of legislation will emerge which will be difficult for traders to navigate. Even large, international tech firms and platform operators mentioned that they found the current consumer law landscape complex, given that some new national rules have emerged. For instance, a major marketplace connecting buyers and sellers but playing an intermediation role only pointed out that some of the transparency requirements in the Modernisation Directive for marketplaces and platforms had previously already been introduced through national legislation in France to identify whether sellers were individuals or professional traders. Traders and their representative associations generally supported the continuation of a harmonised EU approach to regulating unfair commercial practices. They did

not generally favour the introduction of additional, more specific requirements, including extending any national legal rules to the EU. Their preference was to retain the general provision clauses and for a case-by-case assessment to be undertaken as to whether particular practices can be considered unfair, misleading or aggressive.

There was feedback from traders and trader associations as to some specific concerns about the development of national legislation in some areas of unfair practices, including both the risk of regulatory fragmentation (despite the UCPD being a maximum harmonisation Directive), and the risk of unintended consequences. For instance, there were various concerns regarding the cancellation button in German legislation and withdrawal button in relation to distance financial services contracts in the DMFSD. Regarding the **cancellation button**, the main reservations identified by large firms in the digital sector interviewed were that the cancellation button risks being too prescriptive and not suitable for all transactional situations and platforms. Feedback from major players in the provision of apps to consumers was that whilst such a button may be possible for e-commerce websites, it would not be suitable for other types of traders as it would interfere with their design interface in a way that may make the existing cancellation procedure more cumbersome. The German legislation requires several clicks, and controversially does not require the user to be logged in to be able to cancel a contract, whereas some traders interviewed stated that they had designed systems whereby users could cancel contracts at any time both through hardware (systems settings) and through apps. Therefore, a possible cancellation button requirement could make it more clunky than the current user-oriented means of cancelling contracts.

If such a regulatory initiative were to be considered at EU level in future, however, the evaluators note that it could be possible to design regulatory objectives in a way that suits different types of traders and incorporates flexibility in design interfaces. For instance, a legal academic from Spain specialising in consumer and digital law highlighted the point that screenless devices are becoming more pervasive, therefore rules on cancellations may need to vary depending on the type of design interface concerned. ELI argued in their position paper in relation to contract cancellation that “Legislative action at EU level is advisable for two reasons: (1) the protection of the consumer; and (2) the avoidance of legal fragmentation”. Amazon commented in their position paper that there is a need to maintain the level playing field, which implies retaining EU-wide legislation and avoiding national divergence in rules on unfair, misleading and aggressive commercial practices. *“Consumers should be protected in a clear and consistent way across the EU irrespective of whom they contract with or where they contract. The framework should contribute to economic growth in the EU Single Market, establishing a level playing field”*. So long as the objectives are achieved, the design requirements could be left open. Conversely, a legal academic in Germany argued the opposite - that the lack of standardisation in the design of cancellation buttons on ecommerce websites required to comply with the legislation cancellation button led to divergent application, with recurring problems around dark patterns, meaning the problem of the difficulty in cancelling subscriptions has not been resolved despite the button’s introduction.

Regarding the **protection of minors**, the recent adoption of proposed legislation in France to check the age of those using social media when signing up for accounts was mentioned by stakeholders. Some have questioned the practical application of such legislation as children may find ways to circumnavigate the parental controls required for users of social media under-15. However, other stakeholders, such as Ministries in several countries (DK, SE, FI and NL) have stressed that they support age verification as digital addiction and other problems relating to social media usage are prevalent among minors, yet the current level of protection for minors in the UCPD is low.

Whilst ‘age’ is a ground upon which under Art. 5(2), consumers may be considered vulnerable, minors are not mentioned at all in the legislation. Indeed, there is no common agreed definition at EU-27 level as to what is a minor, whether under 15 (in the case of the age verification

requirements in the French law relating to users of social media), under 16, under 18 etc. It should also be noted that whilst all stakeholders agree that consumer protection of minors given their increased vulnerability in certain situations is important, there are widely differing views as to how this objective should be achieved, and whether regulation is needed (at EU level) or if traders can be relied upon to develop tools to provide relevant information and data (e.g. screen time monitoring of usage of phone and individual apps), ensure parental controls are available (e.g. to address digital addiction and problems with bills arising from in-app purchases especially in video games (e.g. loot boxes and virtual items)).

Concerning **influencer marketing**, some Ministries and consumer ombudsmen have debated the issue of whether to introduce national legislation on influencer marketing. In **France**, as noted earlier, legislation was adopted in 2023 to provide a definition of an influencer and distinguish between professional traders and individual amateurs, and to protect minors.

Denmark debated the issue in a working group of the Consumer Ombudsman and it was perceived to be difficult to establish a clear dividing line between professional traders (who might be more clearly regulated and made explicit subject to consumer law) vs. casual influencers. The debate was around whether this should be triggered by having a certain number of followers. The issue around how best to regulate influencers not only relates to how to define an influencer (does this include all content creators), but also the issue of how to define an advertisement in the content of videos. Traditionally, it has been clear what an advertisement is in various media, and how this has to be regulated. However, this is less the case with influencers, where hidden ads may be much more nuanced, depending on the relationship between the influencer and sponsors and advertisers. The section on influencer marketing (2.1.8) has further details about influencer marketing.

The emergence of national legislation – key findings

The proliferation of national legislation on problematic practices in areas such as influencer marketing, subscriptions and the protection of minors threatens to undermine the effectiveness of harmonised EU legislation, especially the UCPD. Such legislation has arisen as national legislators and politicians have been under pressure to address citizens' concerns regarding specific problems in the digital environment in instances where EU legislation provides high levels of consumer protection through the UCPD's general clauses, but there is a lack of detailed rules and a perception among some stakeholders that this may undermine regulatory certainty and/ or constitute a legal gap.

This raises a policy consideration whether some (or all) of the above practices (e.g. loot boxes, influencer marketing, subscription cancellation mechanisms) should be regulated further at EU level through EU consumer law to avoid a patchwork of different national rules emerging that would constitute barriers to the full and effective functioning of the internal market.

As the volume of such legislation increases, this will create increased barriers to trade for traders. There is also a question as to whether such legislation is compatible with EU law, given that the UCPD is a maximum harmonisation Directive (e.g. if hidden advertising is already covered, how far can it be justified that some EU MS have introduced more detailed rules on influencer marketing?).

Whilst the UCPD's general principles-based approach has provided regulatory stability for consumers and traders, there is a trend towards more specific rules in particular areas to address some uncertainties that new business practices and business models may present in the digital environment (e.g. whether there should be stricter rules for marketeers and influencers when marketing products and services to children and teenagers).

3 Assessment of the Fitness Check evaluation questions

This section provides an assessment of evaluation issues structured by evaluation criterion. It should be noted that problematic practices are addressed in the sections dealing with the effectiveness and relevance criteria. This is complemented by case studies in Annex 5.

3.1 Effectiveness

Effectiveness can be defined as the extent to which an intervention achieves its general and specific objectives and contributes to wider policy objectives. According to the 'Better Regulation Guidelines, an evaluation should analyse the progress made towards achieving the objectives of the intervention, looking for evidence of why, whether or how these changes are linked to the EU intervention.

The assessment of effectiveness considers progress towards the achievement of the general and specific objectives of the three pieces of EU consumer law within scope, focusing on the impact on digital fairness. In addition, the extent to which problematic digital business-to-consumer ("B2C") practices have influenced the effectiveness of the Directives is also considered as is the effectiveness of the Directives' application from an enforcement perspective with a particular emphasis on digital markets and transactions. The level of compliance among traders is also considered, given the inter-linkages with enforcement together with the overall effectiveness of the Directives' implementation.

EQ3 – How successful have the Directives been in achieving their objectives and in promoting digital fairness?

Stakeholder views on progress towards objectives were mainly ascertained through interviews and the targeted consultation. Feedback on general objectives (i.e. the dual objectives of high levels of consumer protection whilst facilitating the functioning of the single market) was gathered through interviews, whereas feedback on Directive-specific objectives and those relevant to different aspects of the functioning of EU consumer law in the digital environment was also solicited through the targeted survey.

3.1.1 Progress towards general objectives

Overall, the assessment has found that EU consumer law has been partially successful in achieving progress towards the core objectives of achieving high levels of consumer protection, whilst facilitating the effective functioning of the single market. Specifically in the digital area, the legal framework was found to be broadly fit for purpose, but with a need for more effective enforcement and more specific rules in certain areas where legal gaps and/ or low levels of compliance have been identified.

EQ3(1) – What progress has been made towards the achievement of general objectives?

In terms of progress towards the **general objectives**, these relate to the legal base for EU consumer law under Art. 114 TFEU. These are:

- Achieving a high level of consumer protection across the EU; and
- Contributing to the effective functioning of the internal market.

It should first be reiterated that the definition of these objectives does not explicitly cover the digital environment, although it is implicit that consumer protection should be achieved in the digital arena irrespective of the type of trader or the medium (e.g. websites, platforms, marketplaces etc.) or the type of device concerned (e.g. devices with screens and without).

Overall, the **general principles-based approach** in the UCPD and the UCTD respectively (e.g. commercial practices, contract terms) was seen as having been an effective means of ensuring that consumers are protected from using unfair (including misleading, aggressive) commercial practices or unfair contract terms. Whilst commending the principles-based approach, some stakeholders (e.g. consumer associations, academics, national authorities) did not think that the rules are sufficiently precise enough to ensure they are interpreted in the same way across the EU-27 MS, which is problematic. This was especially noted in interviews but also through other stakeholder consultations, such as the targeted survey.

Whilst **digital fairness is not an explicit objective of EU consumer law presently**, the research has identified good progress towards the objective of high levels of consumer protection more generally, albeit with some legal gaps, for instance due to the updating of other EU laws to accommodate digital aspects (considered in the relevance and external coherence sections). Given that a significant percentage of EU trade takes place in the digital environment, it can be assumed that consumer law is contributing significantly to digital fairness by providing consumers with rights to be protected from unfair, misleading and aggressive practices and from unfair contract terms which exist across different areas of the digital environment, and which are explored through case studies focusing on problematic practices such as subscription traps and aggressive practices.

Overall, whilst consumer law provides a good starting basis for protecting EU consumers in the digital environment, there are **some outstanding challenges** which means that the general objective of high levels of consumer protection has still not been fully achieved in the digital environment. These include:

- The persistence of **problematic practices specific to the application of EU consumer law in the digital environment** (explored in Section 2 on problematic practices, EQ1 and in a series of thematic case studies in annex);
- **Sub-optimal compliance level among traders with existing rules in certain areas** – there remain challenges in ensuring high levels of compliance with existing EU consumer law rules in some areas. Examples are considered in Section 2 on problematic practices, and include for example, the longstanding existence of rules on hidden advertising in the UCPD, but only low-to-medium awareness-levels among influencers of these rules with compliance being lower compared with among other types of traders.
- **Enforcement** – there are **general challenges** in ensuring uniform levels of enforcement across the EU-27 of EU consumer law (as noted in the earlier 2017 fitness check and in this study) but also **specific enforcement challenges** in the digital environment. This is due to multifaceted reasons e.g. the complexity of legal enforcement cases which may cover consumer law and its interaction with other pieces of law, absence of sufficient critical mass of national case law and CJEU rulings in digital sphere. EQ5 considers issues relating to the enforcement of consumer law.
- **The need to strengthen coherence with other recent EU laws, especially those that are digital and data-related.** Whilst coherence-related issues are analysed in detail under that evaluation criterion (see Section 4.5 – coherence), the development of many new pieces of law raises issues around whether consumer law is sufficiently clear regarding some practices that are clearly regulated in other EU laws (e.g. the DSA regulates dark patterns, the GDPR and the DSA regulate the use of sensitive data, including in personalised ad's). A lack of coherence means that it is difficult for the legal framework to be as effective as it might otherwise be.

It was mentioned by many stakeholders interviewed that whilst the Directives within scope (UCPD, CRD and UCTD) have been broadly effective when applied to different digital markets, EU consumer legislation is designed to be **technology-neutral** and is therefore applicable both in an online and offline environment. Moreover, consumer law is also intended to be **channel-neutral** as many traders operate multi-channel and therefore have longstanding experience in applying the legislation both online and offline. The public consultation responses and accompanying position papers and the interview feedback broadly confirmed the findings from the previous fitness check that the body of legislation is fit for purpose and can be applied both offline and online.

However, trade association representatives and some individual traders interviewed expressed concerns that effectiveness of the technology-neutral approach in EU consumer law could be undermined if there continues to be a gradual accretion of new EU legislation and updating of existing provisions in digital markets and services. They mentioned not only the MD but also recently adopted legislation such as the DSA and DMA, as well as laws amended or introduced within the past few years, such as the revised AVMSD, and GDPR. They also highlighted the point that further digital-focused legal requirements and privacy-related requirements on data are being introduced, for example, through the future adoption of a regulatory proposal such as the AI Act, e-Privacy Regulation etc.

The 2017 fitness check also noted that there were some areas where more detailed and specific rules for the digital environment could be warranted. The research conducted through this study broadly confirms the findings from the earlier study in this regard. However, a difference compared with the previous fitness check study is that in the past 5 years, digital markets and services have continually developed and many new regulatory developments and changes have taken place. There is far more relevant EU legislation applicable to traders across different digital markets and services than was the case in the past and consumer law needs to be applied not only in isolation but also in parallel with other EU rules.

This raises a question as to whether **high levels of consumer protection (with digital fairness as an implicit goal within this objective)** can be fully achieved without more specific rules in at least some areas.

3.1.2 Progress towards specific objectives

EQ3(2) – What progress has been made towards the achievement of specific objectives?

Overall, the assessment of progress towards specific objectives found that the Directives have made good progress towards their aims, including in the digital environment.

- **The UCPD (2005/29/EC)** was considered to have been broadly effective since 2005 in protecting consumers against unfair (including aggressive and misleading) B2C commercial practices, whilst contributing to the effective functioning of the internal market. However, there were some specific practices where the UCPD was considered to have been less effective based on perceptions that compliance levels are insufficiently high, such as continuing problems with dark patterns, subscription traps and hidden advertising in areas such as influencer marketing.
- **The UCTD (93/13/EEC)** was considered to have been effective overall by all stakeholders. In particular, the Directive provided strong regulatory stability over 30 years. However, the risks have increased in terms of the lack of transparency in mass market online contracts and the presence of unfair terms. The research conducted into the UCTD to assess the fairness of contract terms found that the increasing complexity and interconnectedness of applying the UCTD together with different pieces of consumer, digital and data law means that new application challenges may arise, for instance, ensuring that standard contract terms are fully aligned with GDPR.

- **The CRD (2011/83/EU)** was generally effective in delivering digital fairness for online distance contracts. Some traders and consumers were concerned however about information overload and whether the approach of requiring ever-more information obligations is the right one. Further feedback from marketplaces and traders was that the 14-day RoW extension to content and services has been more challenging to implement since changing processes and procedures incurred costs.

The Directive-specific specific objectives of EU consumer law were explained in Section 3.1.3 (intervention logic mapping). The degree to which progress has been made in achieving these is now considered.

In the latest Consumer Conditions Scoreboard (CCS) 2023¹¹⁹, the national conditions for consumers with regards to knowledge and trust, compliance and enforcement are analysed, drawing on consumers' experiences in digital markets and services, including perceptions as to how frequently particular issues or problems arise. The CCS 2023 confirms that e-commerce use is highly prevalent among EU consumers in the majority of EU Member States, even if consumers in some countries shop online more frequently than in others, where e-commerce has been slower to take off. Overall, the CCS 2023 found that the proportion of consumers who purchased goods or services online in the past 12 months (71%) was similar to that in the pre-Covid-19 period. This implies that whilst there was a spike in e-commerce during Covid, the level of e-commerce is now back to pre-pandemic levels, but is still very high, representing a significant share of the overall market. The CCS notes that *"purchases are mostly made from retailers and providers that appear to consumers as being based in their own country"*. It should be recalled that EU consumer law, through nationally-transposed legislation, is applicable regardless of whether transactions are cross-border or domestic.

Among the key findings is the observation that as e-commerce sales continue to grow, *"consumers are increasingly exposed to frequent unfair practices online. The three most frequently reported practices were: personally targeted online advertising (76%), hidden advertising in search results (75%) and disingenuous consumer reviews (69%). With regards to online advertising, 94% expressed concerns about it, with 70% worried about inappropriate use and sharing of personal data, 66% about the collection of online data and related profiling without explicit knowledge or agreement and 57% about cookie" installation"*. It can be noted that some of these practices are illegal (e.g. fake consumer reviews on platforms since the MD's entry into application in 2022) and hidden advertising in search results under the UCPD, whereas others may be legitimate business practices, such as personally-targeted online advertising, but bad practice prevails in some cases, such as the use of sensitive data for personalised ads and emotional or psychographic profiling. Personalised ads can also be illegal under the GDPR in the absence of the consent of the user to use and process their personal data for advertising purposes.

The conditions for consumers were not all negative, as 76% of consumers in the CCS 2022 trust that traders respect their consumer rights (this level of trust was similar in most Member States), although a quarter of consumers reported they had experienced a problem when purchasing goods and services in the past 12 months. This level of trust implies that many traders do comply with EU consumer law requirements, although some do not, raising level playing field issues within the single market. Issues around non-compliance with EU consumer law by some traders are considered later in the report and in some of the case studies (e.g. online subscriptions, aggressive practices).

Generally, the UCPD has been an effective Directive since the mid-2000s, including its application in a digital context. However, progress towards the effective application of the

¹¹⁹ The Consumer Conditions Scoreboard is a biennial reporting exercise to monitor consumer sentiment across the EU, as well as in Iceland and Norway. It collects data on national conditions for consumers with regards to knowledge and trust, compliance and enforcement and complaints and dispute resolution. https://commission.europa.eu/document/download/89ea35fe-728f-4749-b95d-88544687583c_en?filename=consumer_conditions_scoreboard_2023_10052023.pdf

UCPD has been undermined in recent years by rapid developments in digital markets and services and the emergence of new types of business practices, whilst relying largely on the general principles-based clauses. Based on interview feedback, whilst many stakeholders were clear as to which specific problematic practices are prohibited – and which are not, the lack of more specific rules in areas such as online subscriptions to combat traps, dark patterns and hidden advertising in a digital context was noted by consumer representative stakeholders, legal academics and some CPAs and Ministries. Traders often did not see the lack of explicit rules on specific business practices as a problem as the general principles-based fairness test is applied on a case-by-case basis and as the guidance highlights specific practices that are prohibited. However, consumer stakeholders perceived that the absence of specific rules in a digital context is causing confusion as to which practices are already regulated. This has led to some degree of regulatory uncertainty for traders and consumers, compounded by the emergence of national consumer rules in some areas in some EU MS.

There were differences of opinion between stakeholders regarding how the UCPD's effectiveness could best be strengthened. There were differing views as to whether more specific rules could be needed in future to enhance regulatory certainty, or whether this could be best addressed through more frequent updating of the (non-legally binding) guidance and/or more proactive enforcement by CPAs. Stakeholder feedback and study team suggestions on the possible way forward to tackle problematic practices more effectively are considered under relevance.

A focus on personalised advertising

The absence of specific rules in the UCPD and CRD on targeted advertising was identified by some stakeholders as an example as to how the Directives' effectiveness could be questioned, considering regulatory developments in other areas, notably through the GDPR and more recently through the DSA's transparency requirements regarding personalised ads and the prohibition of the targeting of personalised ads based on sensitive data or targeting minors. The specific provisions are analysed in the external coherence section.

Personalised advertising is a prevalent practice in the digital economy which may benefit consumers (provided they are informed about it to ensure transparency). According to various stakeholders (e.g. legal academics, consumer associations, CPAs, Ministries), personalised advertising should be allowed provided the existing laws are complied with and there is sufficient transparency, as this is relevant and beneficial to consumers (a point supported by the tech industry), but an effective regulatory approach would require addressing regulatory gaps and inconsistencies.

- Whereas disclosure requirements were included in the DSA for online platforms for ads that have been personalised, this is not the case for the UCPD, meaning a lack of uniform protection for consumers. Whereas large platforms inform them that ads have been personalised and about the basic criteria, this is not the case for other types of traders as no such requirement exists in the UCPD.
- Conversely, through the MD, the new Article 6(1)(ea) of the CRD requires traders to inform consumers if they apply personalised pricing based on automated decision-making. This is applicable to all traders. It is incongruous that there are disclosure requirements for personalised pricing but not for personalised advertising in EU consumer law.
- Moreover, there are issues regarding what should be prohibited. For instance, the fairness of personalised advertising based on information about a consumers' specific vulnerabilities (e.g. digital addiction, such as gambling or gaming) or personal characteristics (e.g. their ethnic or racial origin, sexual orientation, political or religious beliefs) was challenged by several stakeholders (e.g. consumer associations).

It was suggested that clearer and more consistent rules within EU consumer law are needed to prevent ambiguity leading to regulatory uncertainty and undermining consumer protection. There were also calls to ensure more enhanced consumer choice (e.g. an explicit opt-out possibility).

For further research and analysis about personalised ad's, see Section 4.2.7 on problematic practices, EQ13(1) on regulatory gaps and the case study on personalised ads.

Whilst commonly, trader associations and traders interviewed did not object to the specific changes made in the MD to the four underlying pieces of consumer legislation (UCPD, UCTD and the CRD but also the PID), they were concerned about the frequency and cumulative volume of legal changes across EU legislation. This was because many regulatory changes in EU consumer law and in new EU legislation in the domain of digital markets and services and in data law only came into application very recently. Many of these would impact on digital fairness.

Traders and their associations noted that the cumulative volume of regulatory changes both under EU consumer law and in digital law has been quite significant in their view. This had in their opinion left insufficient time to assess the impacts of these regulatory changes at the level of i) individual pieces of legislation and i) regarding their cumulative impacts. There is a need in the view of some trader stakeholders to evaluate the effectiveness of the overall EU legal acquis relevant to achieving digital fairness, i.e. not confining the assessment to consumer law but considering other new digital and data laws, given that traders complying with EU consumer law must comply with a much broader swathe of legislation, much of which includes, at least partially, among its objectives that of ensuring high levels of consumer protection.

The public consultation position paper from Amazon encapsulated the need to await to allow sufficient time for the legislation to be applied and then fully assessed before further regulatory changes are concerned (but with similar comments being made by many trade associations). *“After current legislation has had time to bed-in and operate, a review and impact assessment should be carried out by the EC in the future to assess if EU consumer laws are (i) coherent with each other and other laws, (ii) understood and functioning as expected, (iii) being complied with (and if not, why not), (iv) leading to improvements for the EU Single Market participants, and (v) not introducing disproportionate economic burdens on business or reducing the competitiveness of EU businesses”.*

The UCTD (93/13/EEC) was considered to have been effective overall by all stakeholder types. The UCTD was seen as having provided regulatory stability, given that the legislation has been in place for 30 years. Positive feedback was received from stakeholders interviewed (e.g. Ministries, CPAs, industry associations, traders) regarding the regulatory certainty that the UCTD has brought regarding which standard contract terms can be considered unfair. However, a few stakeholders, especially trader associations, pointed out that as the UCTD is a minimum harmonisation Directive, there are concerns that retaining a system of national blacklists of unfair contract terms could risk national regulatory fragmentation in a single market context. However, there were also stakeholders that supported the continuation of national blacklists, such as the responsible Ministry in Austria, as these enable them to draw on experiences of the most common national unfair contract terms. A broader series of issues regarding how far it is a problem from a coherence perspective that the UCTD is a minimum harmonisation Directive whereas the UCPD and CRD are maximum harmonisation Directives are considered under internal coherence.

Enforcement powers available under the UCTD were strengthened by the MD through greater turnover-based sanctions. The ability to issue increased penalties was welcomed as providing greater potential to enforce the UCTD more effectively. Given the size and reach of digital mass market actors, and their strong market position, in some cases, the asymmetry of information, expertise and bargaining power has been tilted even less in favour of consumers, when entering into a contract. In turn, the risks have increased in terms of the lack of transparency in mass market online contracts and the presence of unfair terms.

Some literature has raised concerns in relation to the level of compliance with the UCTD in online contracts. For instance, research undertaken as part of this study found examples of non-compliance with the UCTD mainly due to contract terms lacking clarity and being ambiguous.

There have also been some legal cases against major tech players in the digital environment regarding unclear clauses pertaining to the effects of data-sharing activities.¹²⁰ An interview with a legal academic involved in the development of a compendium of EU law also mentioned that there is more case law involving the UCTD than for other EU consumer law Directives, again suggesting that compliance has been a challenge for some traders due to unclear standard contract terms.

The specificities of the contractual environment online and of the online presentation of standard terms (e.g. not always easy to locate, or spread across several webpages) does not always give consumers sufficient opportunity to become acquainted with contract terms before the conclusion of the contract either. In some cases, improving transparency in contract terms themselves, and improving their presentation online, are required. Some stakeholders were also concerned about the application of penalties for traders established in third countries that have committed infringements of EU consumer law. Industry representatives did not however mention this issue and were more positive about the UCTD's role and its effectiveness, which was seen as stemming from the fact that the Directive was well-established and well-known, as it has been in place for 30 years, and has provided regulatory stability.

Some specific issues were raised also around the UCTD's complementary role to the UCPD in providing consumer protection in the digital environment. For instance, in relation to online subscriptions, whilst the UCPD prohibits subscription traps as an unfair commercial practice, it was pointed out that the legislation is not explicit on this type of practice. At the same time, the UCTD can apply, given that unfair contract terms may tie in consumers to subscription traps, and if it is proven that the related terms are unfair, they will not be binding on the consumer and must be removed/disapplied and the contract will continue to be performed without the unfair term(s) (as per Article 6(1) of the UCTD). Where the contract cannot continue in existence in the absence of the terms considered unfair, the full contract will be annulled. This is a good example of how different pieces of EU consumer law within scope can be mutually reinforcing in ensuring strong consumer protection in the digital environment.

An aspect of the UCTD's application seen as being especially effective by stakeholders (e.g. Ministries, CPAs) was the unfairness test which remains relevant to the digital environment. Many stakeholders perceived this should remain untouched. Member States' ability to develop national consumer protection rules that go beyond the minimum EU level of consumer protection, i.e. a broader scope of the national rules transposing the UCTD, or more detailed or stricter rules regarding the unfairness of contract terms, was seen favourably by some Ministries who preferred to rely on national case law and to develop their own blacklists or grey lists of contract terms, partially because they said some contract terms are used nationally and are specific to a given Member State, and partly to reflect the fact that contract law is a national competence. Further feedback is provided under an EQ about the UCTD under relevance. This being said, given the cross-border nature of a significant portion of trade online and the emergence of new practices reflected in contract terms, certain stakeholders consider that additional guidance for economic operators is needed beyond the strict requirements of the UCTD (1) on what compliant T&C in digital business should look like (e.g. in relation to consent to collect and use personal data in line with GDPR; or to changes to T&Cs, or to copyright and ownership of consumer-generated content) and (2) how they would best be presented online (interface design).

¹²⁰ Consumer Vulnerability, Digital Fairness, and the European Rules on Unfair Contract Terms: What Can Be Learnt from the Case Law Against TikTok and Meta? M. Durovic and J. Poon. *Journal of Consumer Policy* (2023) 46:419–443

The CRD (Directive 2011/83/EU) was perceived as being generally effective in delivering fairness. Among the three Directives, stakeholders viewed it as being the most strongly digitally-focused, given its focus on distance contracts. However, some stakeholders commented on the different ways in which the Directive has evolved after the MD's introduction, and on the extent to which this had impacted on effectiveness. For example, the MD introduced amendments to the CRD regarding "free" digital services that involve processing personal consumer data, including an extension of the 14-day Right of Withdrawal (RoW) to such cases. Similarly, the Digital Content Directive (Art. 3) also includes new consumer rights regarding contracts for free services¹²¹. There were some concerns among marketplaces and tech industry stakeholders who provide free services (in exchange for personal data) that whilst this requirement had proved challenging to implement and had required costs to change processes and procedures, they were not convinced that there would be benefits for consumers. For instance, a major provider of (free) email services, mentioned that whilst they had complied with the legal changes, this did not necessarily make the CRD more effective, as consumers could already cancel the service at any time, without any need to exercise the 14-day RoW. Moreover, a major online marketplace for e-books had recently instituted the possibility for consumers to cancel their contract within 14 days, provided they had only read a certain proportion (10%) of the book before cancelling. This was only possible, however, through the availability of specific technology and it was observed that it may be more challenging for SMEs to comply with such requirements.

Regarding feedback on the effectiveness of new requirements introduced in the CRD, broadly, they were seen as being effective, given the need for additional regulatory clarity for marketplaces considering their growing commercial weight in European digital markets. The requirement for transparency in online search rankings was seen by consumer associations as being effective and welcome, although some marketplaces (in common with search engines that were required to provide such transparency under the P2B Regulation) mentioned that they had already been making it clear for some time ahead of EU legislation which rankings were paid promotions. Indeed, from a marketplace and platform perspective, closer regulatory scrutiny of search rankings for paid promotions was already anticipated as it had been made clear in the 2016 UCPD Guidance that "the relevant provisions make it necessary for online platforms to indicate search results that contain 'paid placements', i.e. where third parties pay for higher ranking, or 'paid inclusion', i.e. where third parties pay to be included in the list of search results"¹²².

This problem was confirmed through a website sweep undertaken for this study (see Annex 3) which identified a major lack of compliance, especially with the required explanation about the main parameters of search rankings (only 27.2% complied). The results are expanded upon further in the separate parallel report on the application of the MD. The only concern expressed by European and global marketplaces interviewed was the need to keep criteria to determine search rankings relatively high-level, rather than to provide absolute transparency about search rankings' technical parameters. The concern otherwise was that this could lead to unintended consequences. According to a marketplace interviewed, too much disclosure could risk allowing both competitors and potentially malevolent third-parties to manipulate and "game" marketplaces and/ or platforms' ranking systems.

Regarding the additional regulatory changes, such as requiring marketplaces to ensure transparency about the seller's identity, this was seen as an effective approach by consumer representative associations interviewed. This should ensure adequate transparency for consumers. However, some concerns were expressed from this stakeholder category

¹²¹ Art. 3 DCD (scope). This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service.

¹²² COM(2018) 185 final. SWD accompanying the regulatory proposal for the Modernisation Directive.

regarding whether the cumulative volume of information due to transparency requirements could risk consumer information overload, which is especially pertinent in case of the CRD, which entails pre-contractual information obligations.

For instance, BEUC observed in an interview that given the significant challenges that consumers face in digesting terms and conditions and other pre-contractual information, there was a question as to whether consumers will read all the new information responding to transparency requirements introduced. This challenge has been explored in various position papers, including by national authorities, and in previous research. For instance, a BEUC position paper from 2022 on digital fairness¹²³ points to information overload already due to various disclosures being provided to consumers, such as terms and conditions, disclaimers, cookie policies and privacy policies: *“In a digitalised economy characterised by information overload ultimately limiting the cognitive ability of consumers to process and understand such information, even without the possibility to do anything against it except for not engaging with the service provider, further disclosure would be counterproductive”*.

This encapsulates a problem faced by regulators responsible for EU consumer law. The introduction of new transparency requirements through the DSA and the MD focusing on improving transparency for consumers was welcomed by consumer associations, for instance in helping consumers to understand if the ultimate trader is located outside the EU, and where the trader implies they are located, nonetheless, adding further “transparency requirements have limited potential to mitigate asymmetries”, as mentioned by the Netherlands Authority for Consumers and Markets in their position paper. Some traders also alluded to being overwhelmed with transparency requirements, not only in EU but also in national legislation.

Many trader associations were concerned that consumers would not benefit that much as the great majority do not read terms and conditions, or other pre-contractual information in detail and they are unlikely to read additional disclosure-related information either. Some large traders interviewed pointed to an apparently contradiction that some consumer associations have called for simplification of terms and conditions in the form of key information, which whilst also welcoming in principle, they pointed out that this is difficult to achieve in light of the gradual accretion of different EU regulatory requirements which need to be reflected in T&C, plus greater transparency obligations, which multiplies the volume of information being provided to consumers, which most don't read anyway. In other words, consumer and trader organisations sometimes share the same goals, providing clear information for consumers in a user-friendly manner, but in practice, it is difficult to deliver this.

Our research examined how pre-contractual information on the 14-day right of withdrawal is relayed to consumers in the context of distance contracts. One of the principal findings is the continued uncertainties associated with how traders present information. The CRD, with its Articles 6-8, clearly stipulates the information obligations and formal requirements that traders must adhere to for distance and off-premise contracts. These requirements were designed to provide consumers with a comprehensive understanding of the goods and services they intend to purchase, ensuring they are well-informed and protected from misleading practices.

A sweep of websites showed that only a slight majority (54%) of the surveyed websites and apps provided consumers with information about the RoW at the pre-contractual stage. This underscores the fact that a significant portion of consumers might be venturing into contracts without an adequate understanding of their rights to withdrawal. Such gaps, whether borne out of oversight or intention, limit consumers' ability to make informed decisions. In addition, even among traders that do proactively provide RoW information, just 41.7% present the RoW information in a manner that can be categorized as 'clear' or 'very clear'. Concerning

¹²³ BEUC (2022). EU CONSUMER PROTECTION 2.0 - Protecting fairness and consumer choice in a digital economy - https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf

information about the technical procedures required for consumers to notify service providers of their intention to exercise their RoW, a majority (56.5%) of platforms elucidate this procedural information with clarity, while 8.7% that leaves consumers confused. The data sheds light on the diverging ways in which platforms approach and implement the RoW, despite harmonised rules at EU level.

Furthermore, results of the consumer survey highlighted a pronounced communication barrier when it comes to dealing with sellers regarding missing reimbursements. An overwhelming 45% of consumers encountered difficulties in this area either always or most of the time, while an additional 29% faced these issues occasionally. These numbers, when aggregated, suggest that almost three-quarters of the sampled population grapple with some level of difficulty in reaching out to sellers for their rightful reimbursements. The demographic breakdown further emphasizes that younger consumers, particularly those aged between 26-35 and 18-25, experience these issues more acutely. With 52% of those in the 26-35 age bracket and 42% in the 18-25 category reporting difficulties, it raises questions about whether these challenges are due to sellers taking advantage of younger, perhaps less experienced consumers, or if there is an underlying pattern of younger consumers being more vocal and assertive about their rights.

Furthermore, a striking 44% of consumers pointed out the challenges they face in merely notifying traders of their intent to withdraw from a purchase. Again, the issue was more pronounced for the 26-35 age group, with half of them voicing this concern. This not only underscores a possible lack of accessible communication avenues but also suggests a potential resistance or lack of responsiveness on the part of traders. Overall, the analysis underscores a pronounced need for clearer communication pathways and more responsive trader practices, particularly to ensure the younger consumer demographic is not disproportionately affected.

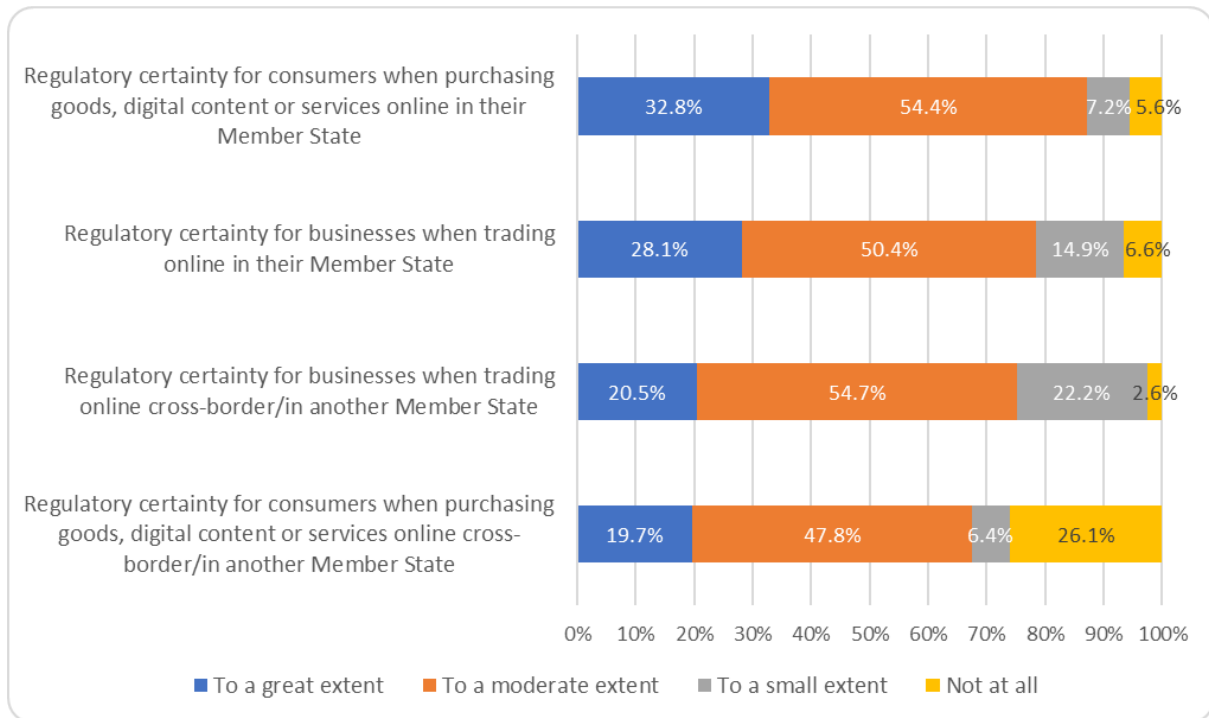
3.1.3 Progress in achieving regulatory certainty

EQ3(3) – How far have the EU consumer law Directives been effective in providing regulatory certainty in the digital environment?

The analysis considered the extent to which the EU consumer law Directives have provided regulatory certainty, and whether there are any areas of the legal framework that have created uncertainty. Moreover, the impact of changes to other EU legislation on ongoing regulatory certainty has been considered.

In the targeted survey, respondents were asked how far the EU consumer law Directives provided regulatory certainty in the digital environment. The results shows that generally, most stakeholders perceive there to be regulatory certainty to a moderate extent.

Figure 3.1 – Overall, to what extent have the EU consumer law Directives provided regulatory certainty in the digital environment? (n=157)



Source: targeted survey

There was a perception that there was greater regulatory certainty when purchasing goods, digital content or services in consumers’ own Member State than cross-border. Whereas 32.8% agreed to a great extent (54.4% to a moderate extent) that there was such certainty when purchasing goods, digital content or services in consumers’ own Member State, this diminished considerably to only 19.7% and 47.8% when purchasing goods, digital content or services cross-border, with 26.1% stating not at all. An interesting finding among traders was that 22.2% of businesses perceived that there was regulatory certainty only to a small extent when trading online cross-border in another MS. This suggests a combination of concerns about possible divergence in application between MS of EU consumer law, but also gold-plating concerns, e.g. regarding the existence of additional national consumer laws pertaining to certain aspects of unfair commercial practices and unfair standard contract terms.

The following table shows the targeted survey responses as to how far there was increased regulatory certainty about the applicable rules across different areas where problematic practices were identified. Mostly, the Directives have increased clarity on the online sales of physical and digital content and services. However, there is perceived as being less certainty in respect of many other issues, such as dropshipping, AI systems (including chatbots), virtual items, scalping outside of event tickets and personalised pricing. The results are perhaps not surprising as these areas are only partially regulated for instance through disclosure requirements (e.g. personalised pricing) or raise concerns among consumers but are not illegal *per se* (dropshipping, personalised ad’s).

Table 3-1 – Regulatory certainty about the different rules (N = 157)

Stakeholders incurring costs (EU consumer law)	To a great extent	To a moderate extent	To a small extent	Not at all
Online advertising (including marketing and personalised advertising)	19.4%	43.0%	25.8%	11.7%
Use of AI systems in the context of B2C commercial practices (including AI chatbots)	19.4%	31.1%	30.8%	18.9%
Virtual items (including loot boxes) and virtual intermediate currencies in digital services, such as video games	19.5%	32.9%	24.4%	23.2%
Personalised pricing	23.6%	39.6%	23.6%	13.2%
Use of scalping (i.e. purchasing of products in high demand using automated tools with a view to resell them at higher price)	23.7%	34.2%	23.7%	18.4%
Subscription contracts for digital content and services	25.0%	46.4%	21.4%	7.1%
Fairness requirements concerning the design of online interfaces (websites, apps)	25.6%	42.7%	18.8%	12.8%
Use of dropshipping (i.e. shop does not hold those products in stock)	25.9%	27.1%	22.4%	24.7%
Provision of “free” digital services (in exchange for consumers’ data)	26.5%	42.5%	20.4%	10.6%
Other personalisation practices (ranking, offers, recommendations etc.)	27.0%	47.0%	19.1%	7.0%
Rules on burden of proof in disputes/enforcement of fairness requirements	28.8%	44.1%	19.8%	7.2%
Online sale of digital content and services	29.5%	52.5%	13.9%	4.1%
Standard contract terms	30.8%	46.7%	14.2%	8.3%
Online sale of physical products and services	40.5%	47.4%	6.9%	5.2%

Source: *targeted survey consultation*

Some consumer associations, Ministries and CPAs were in favour of **retaining the general principles-based approach, but complementing this through the introduction of more specific rules** where especially problematic unfair and/ or misleading commercial practices have been identified, such as dark patterns (deceptive designs in websites and apps, misleading design interfaces and functionalities) and subscription traps. The aim would be to strengthen greater regulatory certainty in certain areas, even if such practices are already (implicitly) covered in the UCPD, and addressed in the guidance.

For instance, it was seen as confusing by many stakeholders that dark patterns are explicitly prohibited in the DSA whereas in the UCPD this is implicit through the general principles-

based clauses and covered in the guidance. Covering dark patterns more explicitly either through a specific article/prohibition in the blacklist and/ or by incorporating digital fairness by design and default principles was seen by many stakeholders (e.g. consumer associations, CPAs, some Ministries) as a means of improving the UCPD's effectiveness by strengthening regulatory certainty for traders and consumers.

However, not all stakeholders shared this view. For instance, many trader associations and individual traders (*interviews, public and targeted consultation position papers*) were in favour of working harder to properly enforce the existing EU consumer law framework. Industry was often in favour of providing regulatory clarity through guidance documents (which should be regularly updated). Guidance was also seen as a means of avoiding compromising on the general principles-based approach, but still providing illustrations as to how the UCPD could be applied in the digital environment. For instance, the 2021 updated guidance includes a dedicated chapter on digital markets and services, and provides examples of relevant case law concerning any prohibited digital practices and/ or practices considered to be problematic, where traders may need further clarity as to how to interpret the law.

Other industry associations were concerned that whilst the EU consumer law framework remains rooted in a general principles-based approach to underpin technology-neutrality, in practice, more specific regulatory requirements have already been introduced through the MD, for instance in relation to transparency requirements for online platforms, scalper bots for event ticket sales, etc. Moreover, trader representative associations, whilst acknowledging the need for some more specific rules in limited instances to address specific problems if sufficiently evidence-based expressed concern that there have been recent legal changes, which imply a direction of travel towards more specific regulatory approaches. The concern was that if this trend continues, this could risk compromising the technology-neutrality and principles-based case-by-case assessment of the potential for consumer harm that has traditionally dominated EU consumer law thinking and practice.

EQ4 – How far are the following rules/concepts still effective and have contributed towards an improved level of consumer protection and trust: (1) the burden of proof and (2) a transactional decision?

EQ4(1) – The burden of proof in EU consumer protection

General caution is needed in reversing the burden of proof, as a long-established legal principle is that the onus is on consumers making complaints (plaintiffs) to prove the evidential basis for their claims. This ensures that a balance is struck between ensuring high levels of consumer protection, whilst protecting traders from spurious legal cases.

Nonetheless, there are currently no provisions regarding the alleviation of the burden of proof to overcome digital asymmetries, despite challenges in opening the black box.

There are a few areas of EU consumer law where there has been a reversal of the burden of proof in specific areas, such as information requirements and proving whether a product was faulty under the Sale of Goods Directive. However, there are no provisions in EU consumer law relating to unfair commercial practices.

This can be contrasted with recent developments in product liability law (strict liability) and in newly-introduced AI liability law (fault-based liability), where rebuttable presumptions are allowed depending on the circumstances of particular cases, but at the discretion of national courts, and depending on evidential rules in civil proceedings.

Even where a rebuttable presumption is allowed, a challenge is that the use of presumptions is dependent on national court systems and administrative rules on the presentation of evidence, which are non-harmonised and differ widely across civil law systems.

Introduction

The burden of proof relates to elements of a legal provision that determine the breach of / or compliance with the law (Prof. Rott, 2024). In EU law, the burden of proof (BoP) has traditionally lied with the consumer as the person that has experienced detriment or harm and needs to satisfactorily demonstrate this to receive redress or to obtain compensation. “Normally, in law, 'he who pleads, proves' applies”¹²⁴. However, in some instances, the burden of proof may be partially reversed under certain circumstances, and/ or national courts may under civil procedures adopt rebuttable presumptions¹²⁵ if it is unrealistic for the plaintiff to provide definitive proof.

Moreover, there is a trend in some EU legislation (proposed and already adopted) where there has been a (partial) reversal of the burden of proof in particular areas.

The reversal of the burden of proof in EU consumer law

A summary of the legal situation in respect of EU consumer law is explained below:

- The **CRD** – whilst the burden of proof generally lies with the consumer for all other provisions, Art. 6.9 places the burden of proof that traders have fulfilled their pre-information duties on the trader rather than the consumer for distance sales (e.g. covering e-commerce transactions and doorstep selling). The burden of proof is reversed in respect of the provision of information during the first six months after a consumer takes possession of a product.
- The **UCTD** imposes the burden of proof on the trader to show that standard terms are individually negotiated and that certain pre-contractual and contractual obligations relating to the requirement of transparency of contractual terms, resulting from Article 4(2), have been fulfilled.¹²⁶ The UCTD leaves the burden to prove other key elements, mainly related to the unfairness of the contract terms, on the consumer.¹²⁷
- The **UCPD** does not regulate the burden of proof *per se*. However, issues around proof and evidentiary standards are alluded to, as well as rules if enforcement authorities need additional information to verify factual claims made to investigate the fairness of commercial practices. In particular:
 - There are considerations in relation to whether ‘proof’ is required in the first place as the fairness test is applied to assess the fairness of commercial practices objectively. This does not always require proof *per se* and / or can be demonstrated by simple means.
 - In other cases, proof would be required to demonstrate unfairness (e.g. proving that an AI algorithm using automated decision-making was biased and constituted an unfair practice).
 - Under Article 11(1) UCPD, Member States shall ensure that adequate and effective means exist to combat unfair commercial practices to enforce compliance with the Directive’s provisions in the interest of consumers. This codification of the principle of effectiveness implicitly touches on the burden of proof and standard of proof.

¹²⁴ <https://www.blatterlegal.com/en/knowledge-base/general-legal/online-consumer-law/>

¹²⁵ A rebuttable presumption is a legal principle that presumes something to be true unless proven otherwise. The burden of proof lies with the party wishing to rebut or disprove, the presumption. A rebuttable presumption is most often found in civil law.

¹²⁶ Joined Cases C-776/19 to C-782/19 *BNP Paribas Personal Finance SA*, paragraphs 83-89.

¹²⁷ This is nevertheless mitigated by the duty of national courts, stemming from the case law of the CJEU, to assess of their own motion whether a contract term falling within the scope of Directive 93/13 is unfair and, if the elements of law and fact already contained in the case file raise serious doubts as to the unfair nature of certain terms, to take investigative measures in order to complete that case file, for example by asking the trader for the evidence necessary to assess whether that term is unfair. See Case C-807/19 *DSK Bank*, paragraphs 49-54.

- According to Recital (25) UCPD, national law determines the burden of proof, although courts and administrative authorities require traders to produce evidence as to the accuracy of factual 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*”. The extent of leeway in terms of how far proof where required may be partially alleviated is considered further below.
- The **Digital Content Directive (Directive (EU) 2019/770)** - according to Art. 12(2) and (3), the burden of proof for the conformity of digital content and digital services with the contract largely falls on the trader.
- The **Sale of Goods Directive (EU) 2019/771** - a reversal of the burden of proof for physical goods (only for defects in delivered goods) is one year from delivery and in cases of continuous supply of goods with digital elements, the period is (a) two years from delivery for a continuous supply during the time period and (b) the entire period of supply in case of a continuous supply for a period exceeding two years.

Developments relating to the burden of proof in EU consumer law

A substantive change was made to the Sale of Goods Directive where a reversal of the burden of proof for physical goods was extended from one to two years for the guarantee period with a one-year period for the reversed burden of proof for product defects in favour of the consumer. However, any such reversal does not relate to the key tenets of EU consumer law relating to protecting consumers against unfair, misleading and/ or aggressive commercial practices and unfair contract terms. Nonetheless, under the next sub-section, there are national consumer rules in some countries that have reversed the burden of proof.

Whereas some pieces of EU consumer law have integrated a reversal of the burden of proof into specific provisions, there are no provisions relating to such a reversal either to prove the unfairness of commercial practices or contract terms. However, in the application of consumer law, sometimes, this is not necessary, as the unfairness text is applied objectively, so the consumer does not always need to provide ‘proof’ in the first place.

As mentioned in the BEUC paper in the chapter on the burden of proof, “*the unfairness test of the UCPD is an objective test. According to Article 5(1) UCPD, a commercial practice is unfair if (a) it is contrary to the requirements of professional diligence, and (b) it materially distorts or is likely to materially distort the economic behaviour regarding the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers. Similarly, under Article 6(1) UCPD, a commercial practice is misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise (...). Thus, the consumer or consumer organisation does not need to prove any kind of subjective element, and in particular no intention to manipulate the consumer*”.¹²⁸

In other cases, the consumer subject to an unfair practice would ordinarily have to prove that a particular commercial practice was unfair as the burden of proof lies with plaintiffs seeking redress. However, in some instances, it would be difficult for consumers to check and provide evidence as to whether particular practices had been applied to them. For instance, the 2024 BEUC paper above gives the example of personalised pricing: “*The first question is whether or not prices are personalised. Clearly, individual consumers will hardly be able to prove personalised pricing, or the use of prohibited criteria in personalised pricing. One could*

¹²⁸ BEUC Anthology: Digital Fairness for Consumers, Chapter 7, Reversal of Burden of Proof, (2024), Peter Rott.

therefore consider shifting the burden of proof ...[to the trader] if there is personalisation”.

Article 11a **UCPD** (as amended by the Modernisation Directive (EU) 2161/2019) provides for a damage claim, if there is a causal link between an unfair commercial practice and damage suffered by consumers. This raises burden of proof issues. As explained in the BEUC study, *“this allows some leeway to the Member States as for the details of the claim. For example, the damage claim can be designed as fault-based, as Germany has done”.*

The use of presumptions under the UCPD is legally contentious from the perspective of how far national courts have discretion to allow assumptions where proof would otherwise be difficult for the plaintiff to establish. For instance, Case C-295/16 *Europamur Alimentación* established that only the practices listed in the blacklist can be presumed to be unfair.¹²⁹ However, given parallels with the PLD, this appears to somewhat a draconian interpretation in the evaluators’ view, not least given the general principles-based approach, with case law examples of unfairness, some of which are included in the interpretative guidance.

In principle, national courts examine the circumstances in specific cases to determine how able the plaintiff is to provide evidence that a particular practice is unfair, misleading or aggressive if there are any barriers to them doing so (e.g. asymmetrical information due to complex nature of digital technologies). However, there is limited case law in the digital environment and limited information about how far courts allow or disallow presumptions in consumer law cases.

Use of rebuttable presumptions

‘**Presumptions**’¹³⁰ are allowed under national law in many Member States, which amount to a reversal of the burden of proof and are rebuttable. This means that national courts can consider the circumstances in a particular case and determine whether it is reasonable to place the burden of proof with the plaintiff. This is the case for instance in respect of the PLD to establish a defect, harm and a causal link between the two. There can be circumstances in which it would be unreasonable to expect a plaintiff to furnish conclusive evidence. Whether presumptions are allowed depends on the circumstances of the case. For instance, if there is an obvious product defect, or if information asymmetries are pronounced and would disadvantage the plaintiff’s case, etc. The proposed PLD revision (COM/2022/495) would formalise recognition of the use of presumptions by national courts. It would oblige the manufacturer to disclose necessary information in court when the injured person has presented facts and evidence sufficient to support the plausibility of the compensation claim, subject to protection of trade secrets and confidentiality. In addition, the revised PLD eases the burden of proof for the injured person by establishing a presumption of defectiveness and causal link under certain conditions. This is easier, however, under strict liability than it would be under national fault-based liability, where the evidential proof would need to be stronger. This is an important point when considering the analogous relevance to the UCPD.

In consumer law, there was evidence of the **partial alleviation of the burden of proof at national level**, as per the following section on national level legal systems, but less use of rebuttable presumptions of unfairness and more asking trader to explain / demonstrate why their commercial practice was not unfair, for instance if it involves a complex technology, product or service.

The use of rebuttable presumptions – but only in specific circumstances, such as when plaintiffs face considerable digital technologies - has now been integrated formally in some EU legislative proposals. It is especially prevalent in EU liability law i.e. in the **Product Liability Directive (PLD)** and the **AI Liability Directive (AILD)**. These are relevant as they

¹²⁹ Para. 42 of the ruling relates to the reversal of the burden of proof: “The more restrictive measures which are prohibited also include, as noted by the Advocate General in points 62 to 64 of his Opinion, the reversal of the burden of proof provided for in Article 14 of the LOCM”, the Spanish legislation concerned.

¹³⁰ In law, a presumption is an “inference of a particular fact”. There are rebuttable presumptions.

are the only examples where there can be a partial reversal of the burden of proof which may also lead to compensation.

- The **Product Liability Directive (85/374/EEC)**. Under the PLD, the burden of proof lies with the injured person, who must prove that the product was defective, that he/she suffered damage, and the causal link between the damage and the defect. Whereas the burden of proof lies with the plaintiff¹³¹, in practice, national courts retain discretion to allow a partial (or even a full) reversal of the burden of proof if there are case-specific circumstances, or information asymmetries which mean that only the trader can provide evidence as to the non-defectiveness of a product. Therefore, rebuttable presumptions were allowed by courts.
- The **PLD's proposed revision (COM/2022/495)**¹³² would explicitly allow courts to use presumptions in complex cases (in case of major information asymmetries between consumers and products) and require businesses to disclose evidential information to consumers. These proposed changes do not amount to a reversal of the burden of proof, but rather to its partial alleviation by allowing courts to use discretion through use of presumptions. According to Article 9(2)(b), the defectiveness of the product shall be presumed if the claimant establishes that the damage was caused by an obvious malfunction of the product during normal use or under ordinary circumstances.
- The proposed **AI Liability Directive (AILD)** - similarly to the PLD, seeks to alleviate the burden of proof in compensation claims pursued under national fault-based liability regimes. The AILD would create a rebuttable 'presumption of causality', to ease the burden of proof for victims to establish damage caused by an AI system. It would furthermore give national courts the power to order disclosure of evidence about high-risk AI systems suspected of having caused damage. The rationale for introducing the AILD is that due to the opaqueness of the technologies concerned, end-users (including consumers) will be unable to understand the underlying design of the AI system and algorithms contained therein, therefore developers of AI systems must explain the functioning of the AI system.

Lastly, outside of either consumer or liability law:

- The **EU non-discrimination directives** provides a reversal of the burden of proof, such as for example the Racial Equality Directive (Dir. 2000/43/EC) in Art. 8.1.

Within the UCPD, one possibility in future suggested by BEUC in their 2024 anthology "Digital Fairness for Consumers" could be to *"allow a rebuttable presumption of an unfair commercial practice where there is an indication of such a practice, based on factual evidence. For example, there could be a presumption that different prices for different persons at the same time are prompted by price personalisation unless the trader proves otherwise"*. This is an interesting suggestion, given the similarity with the longstanding use of rebuttable presumptions in the PLD 1985 (further codified in the recent 2022 legislative proposal, which would extend the potential use of presumptions in certain circumstances to all MS).¹³³

Informational and digital asymmetries

Among the situations in which the burden of proof may need to be alleviated are digital asymmetries. The opaqueness of technologies used in the digital environment, especially AI systems and algorithms, has been identified as a growing problem from a consumer protection perspective, given the growing embeddedness of such technologies across a range of digital

¹³¹ The burden of proof remains with the injured person, who must prove the product was defective, that he/she suffered damage, and the causal link between the damage and the defect.

¹³² Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products COM/2022/495 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495>

¹³³ BEUC anthology "Digital Fairness for Consumers".

markets and services.

In such circumstances, there could be arguments in favour of reversing the burden of proof to overcome digital asymmetries. To some extent, this is already recognised in EU legislation. For instance:

- Whereas the new PLD proposal does not explicitly use digital asymmetries as a term, the legal proposal recognises that there are circumstances in which injured parties would face difficulties due to asymmetries between the producer and the consumer, including due to the opaqueness of some technologies. The analogy with EU consumer law can be noted as the **average consumer** would face challenges in understanding how algorithms work and their role in decision-making when using digital services for instance, when using online platforms and/ or online marketplaces. It would be difficult for such a consumer to provide evidential proof to demonstrate that unfair, misleading or aggressive commercial practices have been perpetrated by a trader, as even for consumer associations and CPAs, opening up the ‘black box’ remains challenging.
- To strengthen contestability, a reversal of the BoP could better allow consumers to investigate how far a particular AI system and/ or algorithm used in a digital platform of service may have used unfair, misleading, deceptive, or aggressive practices. As the trader (and/ or the developer of the AI system on the trader’s behalf) knows their own algorithms best, it could be considered whether they should be made responsible for demonstrating that the system or algo is not unfair.
 - This would be logical given that the ‘average consumer’ is not able to determine themselves or to prove to a sufficient evidentiary standard that a particular digital service is unfair as they are unable to understand or assess the fairness of the underlying technologies, often AI-driven.
 - The same is true of enforcement authorities, as CPAs need significant resources and the support of traders to investigate legitimate complaints made by consumers and will need cooperation from traders to understand and investigate claims of unfair practices.
- Whereas traders expressed concerns regarding the impact of a possible reversal of the burden of proof, some legal academics viewed there as being ways of striking a balance depending on the circumstances of the case and the extent of digital asymmetries. *“EU law takes into account the defendant’s position, in the sense that it wants to achieve a fair balance between the legitimate interests of – in this case – traders and consumers. This would not shift the burden of proof in such a way that it is virtually impossible or excessively difficult for the trader to prove compliance with the law. This is, however, not a problem in the case at hand, as the trader merely would have to show and explain the algorithm applied, which he is well able to do. Indeed, it is for the same reason that in Article 12(2) and (3) of the Digital Content and Digital Services Directive (EU) 2019/770, the burden of proof for the conformity of digital content and digital services with the contract falls largely on the trader”.*¹³⁴

Different means of overcoming digital asymmetries of complex technologies include a full or partial reversal of the burden of proof, and allowing courts’ discretion to require traders to provide rebuttal evidence in specific circumstances if it is unrealistic for the plaintiff to provide evidence to prove their case for legitimate reasons. However, there are also other possibilities, considered under the sub-heading on means for plaintiffs to obtain information and evidence, such as requiring information disclosures, and ensuring that AI systems and algorithms are explainable to improve transparency.

¹³⁴ BEUC Anthology: Digital Fairness for Consumers, Chapter 7, Reversal of Burden of Proof, (2024), Peter Rott.

Means for plaintiffs to obtain information and evidence

It is worth noting the variety of situations in terms of whether proof is required to demonstrate unfairness under EU consumer law, and where this is the case, the extent to which consumers can meet the evidentiary requirements (and have access to sufficient information to do so).

BEUC mentioned in a position paper submission that one of the UCPD's advantages in terms of proof is that consumers do not need to prove that the trader intentionally misled the consumer and that specific economic harms have occurred, but rather demonstrate a failure in professional diligence and duty of care, without establishing intent.

However, it is nevertheless necessary for plaintiffs to prove a particular practice is unfair, misleading or deceptive. In order for consumers to provide 'proof' that there has been an absence of professional diligence and duty of care in the case of an unfair practice, in the absence of a reversal of the burden of proof, there is an issue as to how plaintiffs can obtain information to help prove their case. This is important as the extent to which consumers have means to obtain proof without it being overly onerous is a crucial issue in terms of determining the extent to which – if at all – a reversal (or alleviation) of the burden of proof is needed.

In some cases, courts may recognise that it is **unrealistic for a complainant to furnish 'proof' and under civil law procedures, demand the disclosure of information** (e.g. from a trader, producer or the defendant more generally) to overcome informational asymmetries generally (which could also apply offline) and especially digital asymmetries. As noted by Prof. Rott, in assessing how burdensome factors it is for consumers to provide proof, the **accessibility of evidence** needs to be considered. This includes the information rights of one party but also the documentation obligations of the other party. This may vary between countries depending how far there are any disclosure obligations.

It can be especially problematic for consumers (and/ or consumer associations and CPAs) to obtain evidence **as 'proof' in the case of some aspects of the digital environment, such as opaque technologies**, where there are digital asymmetries. In some cases, this has been mitigated by specific proposed rules in new proposed EU legislation, as highlighted above. There are also examples of alternative means through which users can overcome digital asymmetries without a reversal of the burden of proof, but through improved explainability and transparency in AI-driven decision-making leading to greater digital fairness.¹³⁵ For example, in the **AI Act** there is no reversal of the burden of proof, but there is a **right to explanation for high-risk AI systems**. As the use of AI systems has increased, concerns have grown over their potential lack of fairness and accountability through automated decision-making. Art. 68c of the AIA provides a right to explanation of to any affected person subject to a decision which is taken by the deployer based on the output from a high-risk AI system when it "produces legal effects or similarly significantly affects him or her in a way that they consider to adversely impact their health, safety and fundamental rights".

Burden of proof in national legal systems

As noted earlier, presumptions can be used by national courts in **civil law cases under specific circumstances, depending on the administrative rules in the national judicial system**. Therefore, the extent to which a partial alleviation of the burden of proof can be applied is dependent on national courts, even when there is no general reversal of the burden of proof in EU law.

As per a 2024 paper by BEUC and based on CJEU case law, "according to the principle of procedural autonomy, it is for the domestic legal system of each Member State to designate the courts having jurisdiction and to determine the procedural conditions governing actions at law intended to ensure the protection of the rights which citizens have from the direct effect of

¹³⁵ Alfrink, Kars & Keller, Ianus & Kortuem, Gerd & Doorn, Neelke. (2022). Contestable AI by Design: Towards a Framework. Minds and Machines. 10.1007/s11023-022-09611-z.

Community law”.¹³⁶

The legal academic contributing to the BEUC paper to the chapter on burden of proof found evidence that there is discretion for MS to partially alleviate the burden of proof in particular circumstances. The impact assessment study on the PLD (2021) arrived at similar findings in that there was scope within national procedural rules (civil law) for courts to exercise discretion depending on the level of asymmetry. Procedural rules are a non-harmonised area, given different national legal traditions, variations in administrative and procedural rules and evidentiary requirements etc.

*“Art. 12 UCPD only seems to place a power on national courts or administrative bodies without requiring them to make use of them. Outside the scope of application of Art. 12, Member States appear to be free to introduce alleviations of the burden of proof. An outer limit to that would seem to be primary EU law, in particular the provisions on the free movement of goods and services, which could come into play where national provisions relating to the burden of proof become obstacles to trade”.*¹³⁷

Selected country examples are considered of national rules relevant to the reversal of the burden of proof. However, it should be highlighted that only some of these directly relate to consumer law. Very few examples could be identified from consumer law, as the most frequent use of rebuttal presumptions appears to apply in national tort law in the product liability area.

- **Belgium:** CPAs can require traders to furnish evidence as to the accuracy of factual claims in relation to a particular commercial practice. This can be done in two circumstances: 1) If such a requirement appears to be appropriate due to the circumstances of a particular case (considering the legitimate interest of the trader and any other party to the proceedings); 2) If there is no evidence or insufficient evidence provided by the trader, factual claims can be considered as inaccurate.

Under Belgian law, there can also be a reversal of the BoP in certain circumstances through powers conferred upon CPAs through the CPC Regulation, which sets out the minimum powers that CPAs must inspect, observe, study, disassemble or test goods or services. If there are sufficient indications that a good or service is the subject of an unfair trade practice and CPA agents do not have the ability to carry out the necessary dissection or inspection themselves or the results are insufficiently reliable, companies may be ordered to submit the good or service to dissection or inspection by an independent laboratory or research institution within a specific period and at the company's expenses. This can be considered a partial reversal in that traders can be compelled to prove that their products or services are not unfair, misleading, deceptive, aggressive or harmful. A proportionality test is however required to ensure that the right balance is struck between ensuring consumer protection and not overburdening traders.

- **Czech Republic:** A damages claim for unfair competition should be filed through the Commercial Code rather than the Civil Code, because "where the claimant is a consumer and the conduct in question falls within § 44 to 47 and § 52 of the Commercial Code, § 54 sub 2 of the Commercial Code reverses the burden of evidence so that the defendant has to prove trader conduct constitutes an unfair commercial practice.
- **Germany:** Under civil procedural law, consumer organisations must present the facts of the case in a manner that is admissible in court (principle of submission). According to a respondent to the targeted survey, this is particularly difficult in the case of internal

¹³⁶ See Rewe (n 7), CJEU, Case 33/76 Rewe-Zentralfinanz eG and Rewe-Zentral AG v. Landwirtschaftskammer für das Saarland, ECLI:EU:C:1976:188, para. 5.

¹³⁷ BEUC Anthology: Digital Fairness for Consumers, Chapter 7, Reversal of Burden of Proof, (2024), Peter Rott.

company decisions. It would be helpful to simplify the presentation of evidence, e.g., in the case of fake user ratings. In German medical malpractice law, there is a similar rule to the reversal of the burden of proof in the PLD. If a piece of equipment malfunctions, it can be presumed to be defective, and it is then the trader's obligation to prove that it is not defective instead of the plaintiff.

Germany also has specific rules on the burden of proof regarding influencers through the adoption of a law of June 2021 that came into effect in May 2022. "According to new § 5a para 4 of the Unfair Competition Act, conduct in favour of a third party does not have a commercial purpose if the acting person does not obtain payment or a similar remuneration from that third party. Payment or a similar remuneration is presumed unless the person acting makes its absence credible". The burden of proof for not having obtained payment of any manner is therefore on the influencer.

- **The Netherlands:** According to Article 150 of the Civil Procedure Code (Rv), "the party claiming specific legal outcomes from their presented facts or rights bears the responsibility of proving those facts. In other words, the party making the claim must provide the evidence. Article 150 Rv: "The party claiming the legal effects of the facts or rights which it asserts shall bear the burden of proving those facts or rights, unless a special rule or the requirements of reasonableness and fairness require a different allocation of the burden of proof." However, there are exceptions. For instance, if a product malfunctions, Dutch law presumes that the product was defective with a reversing of the burden of proof. It becomes the responsibility of the seller or manufacturer to prove that the malfunction was not due to their fault. If they fail to provide proof, they must either repair the product free of charge or present evidence that the consumer mishandled the product.¹³⁸
- **Spain:** In Spain, there has been a system of the reversal of the burden of proof since the 1940s in product liability. This has become the general rule, with few exceptions. "Once a claimant has established the action or omission of the defendant, the damage sustained and the causal link between them, the fault of the defendant is rebuttably presumed and the burden of proof is reversed". However, it is noted that an exception is medical malpractice where the BoP still lies with the plaintiff.¹³⁹
- **Sweden:** National legislation has been in force for the previous 2 years shifting of the burden of proof onto traders. Swedish law is based on the "principles of the mode of proof and admissibility of evidence. Following a detailed assessment of the case, the court must decide what has been proved. Certain rules on the admissibility of evidence have been established in case-law, including in relation to where the burden of proof lies. A rule, although there are exceptions, is that "anyone who asserts something must also prove it. If one party has found it easier to secure proof of a certain fact, the burden of proof is often placed on him or her. If a party has found it difficult to produce evidence of a certain circumstance, this may also be of significance for establishing where the burden of proof lies".¹⁴⁰

A general finding is that national civil law rules differ regarding whether there is any (partial) reversal of the burden of proof but this remains relatively uncommon in applying national consumer rules. In contrast, the use of presumptions is common in the application of EU strict liability rules and national tort law. However, this reflects the longstanding tradition that the burden of proof can be reversed in certain circumstances namely affecting the burden of

¹³⁸ Burden of proof and its reversal in Holland - <https://www.maak-law.com/evidence-in-dutch-civil-law/#:~:text=Here%2C%20the%20burden%20of%20proof,the%20consumer%20mishandled%20the%20product.>

¹³⁹ https://www.biicl.org/documents/262_overview_-_spain_jan.doc

¹⁴⁰ Taking of evidence and reversal of the burden of proof, Sweden (2023), European Justice. https://e-justice.europa.eu/content_taking_of_evidence-76-se-maximizeMS_EJN-en.do?member=1

producing evidence for the plaintiff.¹⁴¹

Case law – reversal of the burden of proof

The 2024 paper by BEUC mentioned earlier¹⁴² notes that in individual cases, the principle of effectiveness may require certain alleviations to the burden of proof. For instance, the Court of Justice held in the case of *Danfoss* in relation to equal pay between women and men that it was difficult for the female employees involved in the case to definitively prove that gender was the main ultimate explanatory factor underlying pay differentials as individual employees do not know which precise criteria are being applied to them to assess their performance.¹⁴³ To show that practices in the matter of wages does not systematically work to the disadvantage of female employees, the employer had to indicate how they have applied the criteria and will be forced to make the system of determining pay transparent. The burden was put on the employer to prove that their remuneration practices were non-discriminatory.

A second example of case law cited in the same BEUC paper was in consumer credit law (CA Consumer Finance). The question arose whether and how the consumer could prove that the creditor has breached their obligation to assess the consumer's creditworthiness. In relation to the burden of providing the non-performance of the obligations laid down in Articles 5 and 8 of Directive 2008/48 laying with the consumer, the CJEU found that the consumer did not have the means at his disposal to enable him to provide that the creditor first did not provide him with the information required under Art. 5 and secondly did not check his creditworthiness.¹⁴⁴

The 2024 BEUC research paper also notes that “there are unfair commercial practices that do not work with (openly) visible or otherwise recognisable unfair features, such as the undisclosed personalisation of prices. In such a situation of digital asymmetry, the principle of effectiveness as codified in Article 11(1) UCPD may apply. The situation is comparable to the ones mentioned in the two pieces of case law considered, *Danfoss* and *CA Consumer Finance*.”

Whilst the case law presented above is useful in relation to the question of the reversal of the BoP in different EU legislation, it does not appear that there has been much case law relevant in demonstrating how and where the burden of proof should be alleviated due to digital asymmetries. However, there has been an explosion in the use of such technologies, so it is possible that case law emerges in the medium term.

Stakeholder feedback on the burden of proof

Several stakeholders shared considerations regarding the concept of the partial alleviation of the burden of proof in their feedback and what this may mean in practice. For instance, in a BEUC position paper on the Proposal for an AI Liability Directive, BEUC points out that “merely alleviating the burden of proof will not solve the problems consumers face when claiming compensation for harm caused by an AI system. Even if consumers benefit from the presumptions introduced in Article 3 and 4 AILD, they will still face significant challenges to substantiate their claims”. BEUC advocates for a reversal of the burden of proof such that consumers should only have to prove the damage they suffered and the involvement of an AI system, rather than the causal effects.

A similar set of considerations was made in the *Impact assessment of possible future revisions*

¹⁴¹ Vanderbilt Law Review Vanderbilt Law Review Volume 21 Issue 2 Issue 2 - March 1968 Article 1 3-1968 Presumptions, Burden of Proof and the Uniform Commercial Code Presumptions, Burden of Proof and the Uniform Commercial Code W. Harold Bigham, <https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=3509&context=vlr>

¹⁴² BEUC Anthology: Digital Fairness for Consumers, Chapter 7, Reversal of Burden of Proof, (2024), Peter Rott.

¹⁴³ ECJ, 17 October 1989, Case C-109/88 *Danfoss*, ECLI:EU:C:1989:383.

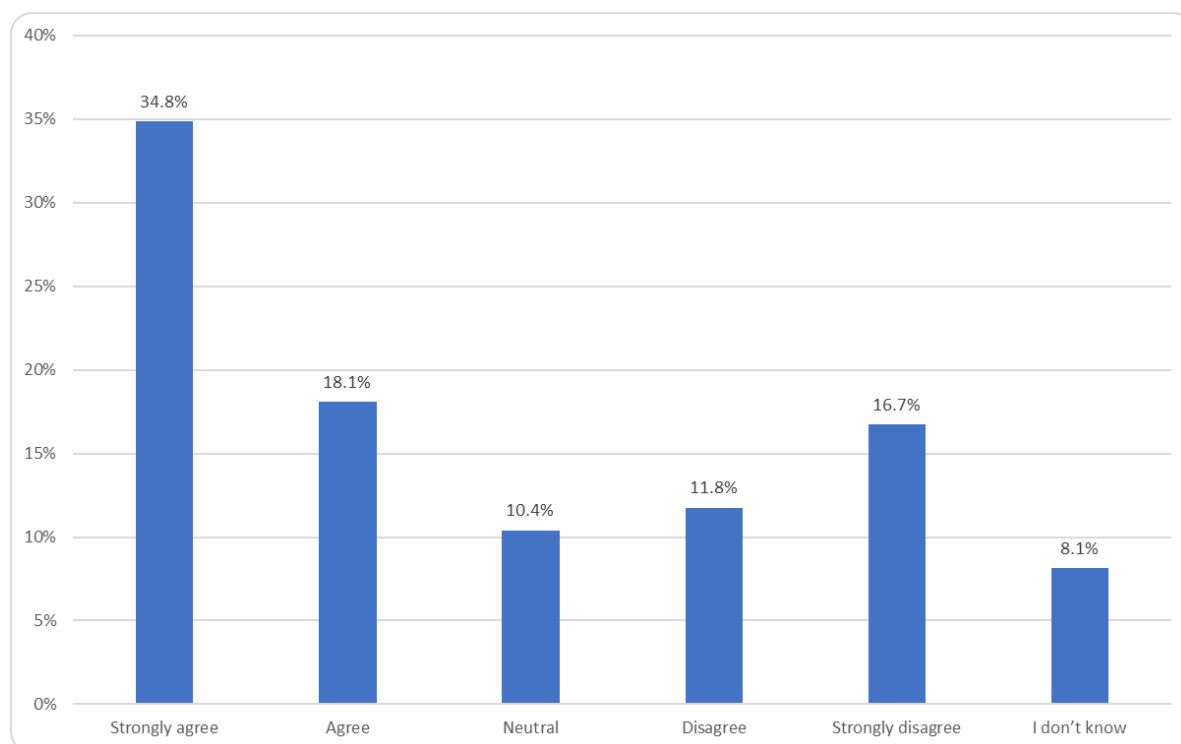
¹⁴⁴ See CJEU, 18.12.2014, Case C-449/13 *CA Consumer Finance SA v Ingrid Bakkaus and others*, ECLI:EU:C:2014:2464, para. 27.

of the *Product Liability Directive*¹⁴⁵, which led to a proposal for a recast Directive in 2022.¹⁴⁶ Presumptions were already used by national courts to acknowledge that consumers face informational asymmetries compared with producers in knowing about the characteristics of a product (today, increasingly digital products, or AI systems).

The above examples show that there have been partial or full reversals of the burden of proof in EU law, but only in specific circumstances. However, any changes to the burden of proof were seen as being controversial by traders. There were concerns that a longstanding legal principle under both EU and national law is that it is up for the person seeking remedy to prove that they have suffered harm and/ or detriment. Even under liability laws, it is still generally the plaintiff that is required to provide evidence to demonstrate proof, unless there are specific legitimate circumstances whereby there should be a rebuttal presumption leaving it for the producer to disprove by furnishing evidence.

Respondents to the **public consultation** were asked whether the burden of proof should be shifted to the trader in certain circumstances (e.g. when only the company knows the complexities of how their digital service works). Overall, 34.8% strongly agreed, 18.1% agreed, 10.4% were neutral, 11.8% disagreed and 16.7% strongly disagreed. A further 8.1% indicated “don’t know”. However, as shown after the graph, there was strong divergence in views between traders and consumers.

Figure 3.2 – The burden of proof of compliance with legal requirements should be shifted to traders in certain circumstances (e.g. when only the company knows the complexities of how their digital service works). (n=221)



Public consultation

¹⁴⁵ *Impact assessment of a possible revision of the Product Liability Directive*. See European Commission SWD - <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0316> and study to support an *Impact assessment of a possible revision of the Product Liability Directive* (PLD), CSES, Wavestone and CSIL.

¹⁴⁶ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products COM/2022/495 final - <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52022PC0495>

Whereas 58.3% of consumers and their associations strongly agreed and a further 30.1% agreed with a possible reversal of the BoP, 25.9% of trader associations disagreed and a further 43.2% strongly disagreed. For other stakeholder types, there were insufficient responses to be able to generate meaningful data on a disaggregated basis.

Some stakeholders provided qualitative feedback on the topic of the burden of proof in their public consultation position papers on this topic, which complements the survey data presented earlier.

The main arguments advanced by stakeholders such as EU consumer organisations and some national Ministries in favour of alleviating the BoP are that in the digital environment, consumers face a variety of digital asymmetries, which are partly informational, but also structural. Digital asymmetries may, depending on the circumstances, be such that they worsen the informational imbalance between traders and consumers, especially in the case of some new technologies, such as AI and the use of algorithms, where it is difficult (if not impossible) for the consumer or their representatives to develop the same level of understanding as the trader as to whether algorithms lead to unfair or aggressive practices. In their position paper in response to the fitness check, BEUC supports placing the burden of proof on traders to demonstrate their commercial practices comply with EU law.

BEUC also makes the argument that digital asymmetry also affects enforcers at several levels. This is notable in the dimension of **knowledge** (e.g. in the case of the necessity to penetrate through opaque algorithmic environments), **architectures** (where the traders' choice architecture evolves quickly and may be a far cry from the original version at the time of the investigation) and **resources**, as building up evidence for effective policing of complex digitalised environments requires disproportionately large expenditures on the part of enforcers.

The **European Law Institute (ELI) position paper** considers that the "opacity of digitalisation is an obvious candidate for such a shifting of the burden of proof". This has already been seen in the proposed PLD and AI Liability Directive, but could be reflected in the UCPD in future, given that technologies such as AI are especially difficult for an average consumer to understand whether a particular practice using a particular technology disadvantage them or not. However, an issue for debate here is whether it should be courts to determine whether the BoP should be reversed, exercising discretion depending on the case-specific circumstances and particular technology and degree of digital asymmetry involved or whether there should be a more universal reversal of the BoP in all cases of digital asymmetry. ELI makes a practical suggestion as to how a potential reversal of the BoP could be dealt with in a possible future updating of the UCPD. *"Only upon establishing a potential breach of law would the burden of proving compliance with the law be shifted to the trader – or to the online platform provider – who would then have to explain, for example, the functioning of the algorithm it uses."*

In an interview with a **legal academic from Italy**, the issue of how the average consumer is vulnerable in a digital environment because the environment is more structurally hostile than offline was stressed. In such a context, the trader should explain how their commercial practices and website design approaches are compliant, as they understand the rationale underlying the design whereas the consumer and enforcement authorities do not have the same level of information accessible and understanding. In their view, the burden should be shifted to traders if either a consumer or an enforcement authority has a reasonable suspicion that the business practice or website design is unfair.

A collective response from the **Danish Government** (given several Ministries are responsible) notes that the issue of the **reversal of the burden of proof could help not only consumers but also enforcers**, who must develop an understanding of sophisticated technologies to understand whether EU consumer law has been infringed, and to support any subsequent

enforcement actions, which is very time-consuming, resource-intensive, and costly. As per the Danish response: *“The UCPD must reflect the fact that digital asymmetry also affects enforcers. Pinpointing unlawful behaviour is made more difficult as authorities can have trouble identifying a single transactional moment for examination. Lengthy and resource-consuming investigations can be very difficult from an evidence perspective and enforcement authorities can have a hard time keeping up with platforms that are constantly updating and making use of new online choice architecture”*. A reversal of the BoP should be applied in the UCPD *“whenever there is evidence of digital asymmetry, which materially distorts the decision-making autonomy of the consumer”*.

Traders expressed **concerns regarding the impact of a full or partial reversal of the burden of proof in consumer law**. Among their main concerns are the fact that the onus in law has historically been on the consumer (or in the case of collective actions, on a Consumer Protection Authority) to prove that a practice is unfair. They worry therefore about the potential for an increase in legal cases and for the potential for spurious or fraudulent cases.

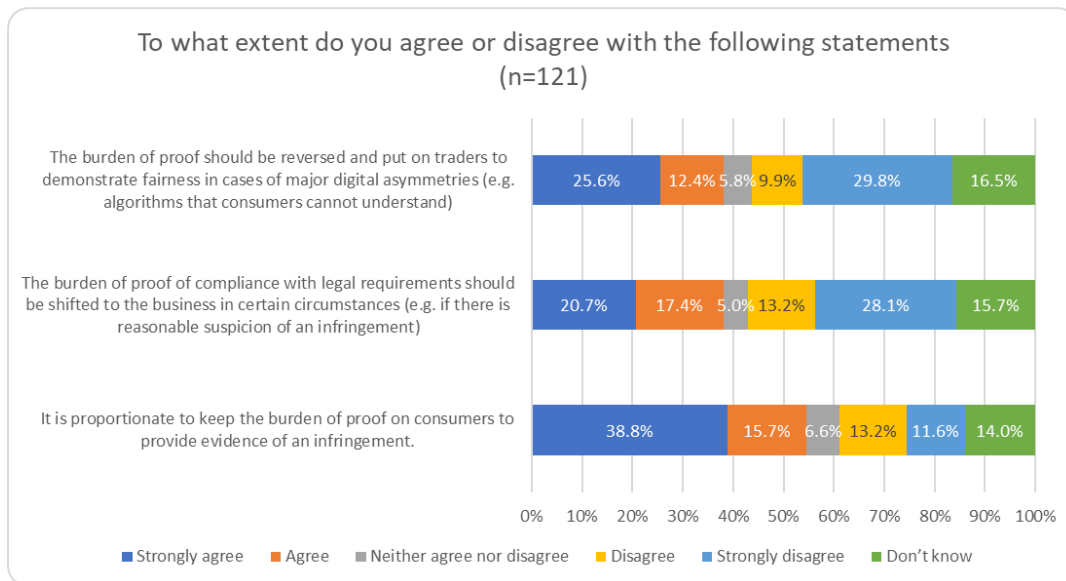
For instance, in its position paper, **Ecommerce Europe** notes that trust is paramount for e-commerce, e-merchants need to provide a safe and trustworthy environment to gain and retain customers. Shifting the burden of proof would undermine good faith and loyalty as core principles of consumer law. Rather than assuming as a basic principle that traders are not acting in good faith, two alternative courses of action could improve consumer protection 1) enforcing existing regulation towards all actors, and 2) encouraging consumer protection authorities (CPAs) to establish a close dialogue with traders, to inform and guide businesses in applying legislation when needed (especially for small traders). Ecommerce Europe fears that a shifting of the BoP could lead to unsubstantiated claims, as many issues could be considered as **"complexities" in digital services**.

Amazon noted that any further obligations imposed on traders should be universal (as mentioned above, a level playing field in consumer rights and protection is crucial), proportionate (not too burdensome on traders) and justified by the desired outcome (consumer protection). These rules should be enforced across the board (not just on large traders) and the compliance measures verifiable.

DOT Europe argued that any reversal or change to the burden of proof should be carefully considered, as it could risk frivolous claims being made. They also considered that existing EU consumer law instruments have introduced a de facto shift in the burden of proof for specific issues and that further adjustments are not justified at this stage. They note that *“products should not be presumed detrimental or “unfair” for consumers simply because they are digital and/or complex”*. **Independent Retail Europe** considered that a reversal of the burden of proof/argumentation equates to a presumption of non-compliance by the trader and should therefore be avoided. Furthermore, the risk that this approach could have a disproportionate impact on SMEs was also noted. A stakeholder representing the **direct selling industry** stated (targeted consultation) that *“the reversal of the burden of proof would disproportionately burden economic operators and structurally weaken redress options offered at no or low cost”*.

As shown in the graph below from the targeted survey, stakeholders’ opinions on the reversal of the burden of proof were divided, as was also the case in the public consultation presented earlier. Whilst 25.6% of stakeholders strongly agreed that the burden of the proof should be reversed and put on traders to demonstrate fairness in cases of major digital asymmetries, 29.8% of the respondents strongly disagreed. However, the survey included a higher percentage of respondents representing traders.

Figure 3.3 – To what extent do you agree or disagree with the following statements regarding the burden of proof? (N = 121)



Source: Targeted consultation

Overall, the stakeholder consultations and literature review point to valid argumentation regarding the possible reversal of the burden of proof in EU consumer law, either in all cases in the digital environment, given the nature of digital asymmetries, or at least in those instances where the technologies concerned are opaque, such as the use of algo's that would make it impossible or disproportionately difficult for the average consumer or CPAs to overcome structural, technological and informational digital asymmetries.

Conclusions – burden of proof

EU consumer law has reversed the burden of proof in some areas (e.g. pre-contractual information provision, defects) but not in relation to the fairness of commercial practices within the UCPD. For cases requiring substantive proof from consumers in relation to unfair practices in the digital environment, problems of digital asymmetries remain prevalent. This means there are risks that consumers are unable to obtain adequate redress in some contexts in the digital environment, for instance, proving that digital technologies, such as the way in which algos within AI systems make decisions, are unfair.

In other EU legislation, both digital law and product liability law, there are already examples of partial reversals of the burden of proof to address digital asymmetries for complex digital technologies, such as the use of AI systems and algos (e.g. in the proposed AI Liability Directive and Product Liability Directive). In the AI Act, there is no such reversal, but an emphasis on strengthening information provision to users through explainability.

A reversal of the burden of proof would represent a potentially significant change to the longstanding requirement for complainants to demonstrate evidence that consumer law has not been complied with. However, in circumstances where there are considerable digital asymmetries for consumers, alleviating the burden of proof should be considered to strengthen digital fairness and address deeper informational imbalances between traders and consumers in the digital environment.

The average EU consumer is not able to understand complex algorithms (despite efforts to strengthen transparency and explainability), given a lack of knowledge about these technologies and how they work. Responsibility for the explainability of use of complex digital technologies, such as AI systems and the working of algos should lie with the trader.

There would still need to be adequate protection for traders. This could be achieved by ensured that any presumptions regarding the unfairness of commercial practices in the

digital environment made by courts would be rebuttable by defendants, and secondly, ensuring that any disclosures respect IPR concerns (as per the PLD).

A dual approach could be considered within EU consumer of alleviating the BoP in specific circumstances and strengthening access to information through disclosures and explainability. This would better enable consumers to contest decisions made using technologies considered opaque for the average consumer. Lastly, improving contestability through transparency and explainability is a general trend in EU digital law and consumer law needs to catch up in this regard.

EQ4(2) – How far is the concept of a ‘transactional decision’ in EU consumer law working effectively? Does this concept sufficiently capture commercial practices in the attention economy?

This EQ explores whether the classical interpretation of a “transactional decision” relating to purchase decisions is outdated and whether it may be necessary to codify in EU consumer law the statements in the UCPD Guidance that a transactional decision also covers other actions by consumers that are related to the transaction, such as scrolling, using a service, clicking links, viewing ads etc.

Article 2(k) of the UCPD defines 'transactional decision' as "any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting".

The UCPD's general provisions (Articles 5 to 9) cover unfair, misleading and aggressive commercial practices which are capable of distorting consumers' economic behaviour, thereby causing or being likely to cause them to take a transactional decision that they would not have taken otherwise. There have been very few **examples of UCPD-related case law concerning the concept of a transactional decision**. According to legal academics consulted, the most influential CJEU ruling is the Trento-Sviluppo legal case.¹⁴⁷ The court clarified that a 'transactional decision' covers not only a consumer's decision whether to purchase a product, but also any decision directly related to that decision, for example the decision to travel to and enter the shop. The Commission's UCPD Guidance goes even further in suggesting that the concept of transactional decision should cover decisions such as:

- Spend more time on the internet engaged in a booking process;
- Decide not to switch to another service provider or product;
- Click on a link or advertisement online;
- Continue using the service by browsing or scrolling.

The transactional decision test is necessary for proving an infringement of Articles 5-9 of the UCPD. Only the blacklisted practices in the Annex do not require proving an impact on the transactional decision.

Article 5(1) of the UCPD provides a general prohibition on unfair commercial practices, whilst Art. 5(2) explains when a commercial practice may be unfair in the context of a transactional decision. A commercial practice shall be unfair if: (b) it materially distorts or is likely to materially distort the economic behaviour regarding the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers". "To materially distort the

¹⁴⁷ Case C-281/12 (Trento Sviluppo and Centrale Adriatica Soc. coop. arl v Autorità Garante della Concorrenza e del Mercato - <https://curia.europa.eu/juris/liste.jsf?num=C-281/12&language=EN>)

economic behaviour of a consumer” is defined as meaning “using a commercial practice to appreciably impair the consumer’s ability to make an informed decision, thereby causing the consumer to take a transactional decision he would not have taken otherwise”.

Article 7(5) of the UCPD clarifies that information requirements ‘shall be regarded as material’, with sectoral information requirements relating to misleading commercial practices also referenced in Article 7(6) which relates to a whole raft of other EU sectoral legislation, covering areas such as financial services, the health sector and food sector. The guidance states that “failing to provide such information can qualify as a misleading commercial practice under the UCPD subject to the **general transactional decision test**, i.e. if the omission causes or is likely to cause the average consumer to take a transactional decision they would not have taken otherwise. If this information is not received prior to the consumer making a transactional decision, then the contract can be considered null and void.¹⁴⁸

Articles 8 and 9 of the UCPD regulate aggressive practices. Article 8 states that a commercial practice, “shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to **take a transactional decision that he would not have taken otherwise**”.

Dark patterns are especially relevant in this context, since their objective is to make a consumer take a transactional decision they would not have taken otherwise. In the 2022 behavioural study on dark patterns for the European Commission¹⁴⁹, an online behavioural experiment tested the impacts of unfair practices on consumers’ decision-making in six Member States (Bulgaria, Germany, Italy, Poland, Spain, Sweden). The experiment demonstrated whether the exposure to dark patterns leads consumers to make choices that they would not have made otherwise, i.e. whether it induced a violation of rationality and satisfies the “transactional decision test” of the UCPD. The results from the study by Open Evidence showed that dark patterns labelled as “hidden information”, “toying with emotions”, and “toying with emotions combined with personalisation” had an impact on the consumers’ transactional decision and led to inconsistency with their preferences. The experiment also revealed that not all consumers are equally susceptible to the effects of these practices. The results revealed that, in general, vulnerable consumers were more likely to make inconsistent choices (50.89%) than average consumers (47.24%) when exposed to dark patterns. Regarding structural vulnerabilities, the results showed that some sub-groups of the population may be more likely to make inconsistent choices, such as older participants and those with lower education levels (10% significance level for both categories).

Herbert A. Simon first coined the term “attention economy” in the late 1960s to refer to the economic impact of the information overload issue. However, as the United Nations noted in a study on the subject, the concept has gained popularity due to the emergence of the internet, which has made content (supply) more voluminous and readily available, with attention becoming the limiting factor in information intake.¹⁵⁰

The attention economy is based on the commodification of the consumer’s engagement with the platform in question. A complex web of devices intended to seize, maintain, and profit from the consumer’s attention is at the heart of the attention economy. To keep consumers interested, digital platforms like social media sites and news sources combine psychology and

¹⁴⁸ “DARK PATTERNS” AND THE EU CONSUMER LAW ACQUIS - Recommendations for better enforcement and reform. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patterns_paper.pdf

¹⁴⁹ Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>

¹⁵⁰ https://www.un.org/sites/un2.un.org/files/attention_economy_feb.pdf

technology. A crucial part of this is played by algorithms. They customise material for individual users based on past behaviour with the goal of giving the user the most interesting and pertinent information. These self-learning algorithms improve the way the content is delivered, tightening the loop of engagement. The current attention economy, a byproduct of the digitalization of the economy, permeates every aspect of our everyday lives and can have significant societal economic and political impact.

On the social side, a substantial impact on the human psyche is caused by the loss of individual control over their own personal data, which affects people's views, how they relate to the physical world, and creates a feeling of information overload. Overload of information makes humans more susceptible to making poor decisions, as it reduces mental capacity. This is because people after being exposed to excessive information tend to become “highly selective and ignore a large amount of information or give up and do not go beyond the first results in many cases” (Kashada et al., 2020 p.56”).

Examples of some areas of the attention economy mentioned in the UCPD guidance are now examined. These relate to actions by consumers that are not paid, but involve users spending their time (and providing data) in exchange for accessing services.

The Danish government in their 2023 position paper on digital fairness mentioned several practices that they perceive as unduly influencing transactional decisions, such as retention mechanisms that result in consumers spending excessive time on platforms. Design practices that automatically load and display additional content without requiring the user to specifically request it or precompile it, such as **infinite scrolling and auto-play on social media** and similar mechanisms, can cause unwanted time-loss as it eliminates natural decision points. Similarly, mechanisms that reward users for uploading content or sharing messages can make users spend more time on platforms than they would have otherwise. Recommended content can, however, also enhance the user experience and lead consumers to discover new content within their fields of interest. However, when the consumer is offered new content without the choice to easily opt out, the practice could be considered an undue influence in their view. This is particularly true, when it comes to children, who do not have the same skills to manage their time and interaction with platforms.

The **EP's IMCO Committee own initiative report on addictive design**¹⁵¹ in 2023 recognised the problem of digital addiction and the advertising-based free service model inherent in the attention economy. The IMCO report mentions upfront the adverse health effects (including on mental health and attention spans) of digital addiction associated with excessive screen time generally and/ or more specifically on social media.

There is however a question as to how feasible it would be to prohibit such practices altogether. The social media industry has argued that some design features such as infinite scrolling are preferred by younger age cohorts. However, this is not to suggest that digital addiction is not a serious problem with considerable societal and health consequences. An alternative advocated by platforms interviewed is to provide consumers with user control options to turn off settings such as autoplay of videos which can be disabled. However, whilst some platforms have put users in control, updated versions of some extensively used platforms have replicated the scrolling features of other platforms. Therefore, whilst tools for consumers to make their own choices have increased, equally, app and platform design interfaces have sometimes gone in the opposite direction to capture more of users' time which increases digital addiction. A link should be made here with increased personalisation of algo's that shape infinite scrolling. In some ways, this problem is a more modern version of earlier debated issues around the use of notifications as a retention mechanism when users

¹⁵¹ European Parliament IMCO (2023) Final report on Addictive design of online services and consumer protection in the EU single market.

(including minors and children) are not using the app. This raises a question whether the problem can be adequately dealt with through self-regulation.

It can also be noted that there are several specialist apps to tackle the problem of smart phone and social media addiction provided by third parties, such as Lock Me Out, Screen Time, Digitox etc. However, this requires consumers to acknowledge that they have a problem, as opposed to tackling the problem at the platform level which could be more effective. Notwithstanding, platforms argued that by placing users in control of their social media feeds through settings / control panels, they can provide a compelling UX (User Experience including design aspects) in a way that allows consumers to remain in control.

In the attention economy revenue can be calculated as a function of clicks, time spent and engagement with online advertising of a specific platform. In the attention economy, every second counts and can be beneficial to companies and platforms. Research shows how more attention means more sales; therefore, this massively incentivises brands and platforms to re-evaluate their content and placement strategies. Engagement with a platform, clicks and reactions are the currency at the basis of content monetization. With the advent and popularity of social media platforms, content monetization is the goal of content creators, influencers, and platforms themselves. This way of leveraging content usually monitors the number of clicks received to a link or a post and, therefore, is based on the ability of the creator to grasp the consumer's attention and time. As BEUC pointed out in their position paper, in systems producing revenue from user attention and engagement, often reinforced by behavioural inferences, personalization may take the form of offering clickbait content that the profiled individual is most likely to respond to, with negative emotions like fear or anger being the most useful commercially and the easiest to invoke. Interestingly, evidence shows that sophisticated traders are aware about such psychological biases that can get exploited by ranking algorithms but typically choose to monetise them instead of counteracting them.

Digital advertising has surpassed TV and online video as the fastest growing ad format. The immense potential of digital and contextual advertising is enabled by the attention economy. Some stakeholders suggest that contextual ads proved to be an effective format in maintaining a viewer's attention, which implies that they can drive more sales than traditional formats of advertisements. In addition, contextual advertising allows to reach the desired consumers without the use of cookies. This specific approach is projected to be strongly impacted by the development of AI technologies.

Regarding the time spent on social media platforms, a significant issue is the **pushing of content on feeds that the user has not signed up for** which is time-consuming even if the user can opt out by clicking that they do not want to see some content pushed at them. This nonetheless puts the emphasis on users to spend their time opting out rather than a more consent-driven approach that would require opting in in the first place (push vs. pull). An industry counterargument during interviews with platforms was that these services are often "free" and paid by users' time and advertising and they have invested in making tools available to control user experience. Moreover, consumers have an option to pay for a premium ad-free service (though how far unwanted content can still be pushed may vary). The meaning of choice as regards unwanted content is an issue that has not been explored much in EU studies, but research could be undertaken in future. If the volume of requests as to whether particular types of videos on a feed is such that the consumer gives up as it is highly time consuming to reject them all, this raises the issue whether it is a genuine choice.

Considering the challenges described above, several stakeholders see a need for adapting the legal framework. For example, **BEUC** considers that the definition of 'transactional decision' in the UCPD should be updated to follow the revised UCPD Guidance, to include transactions where the behaviour of the consumer is connected to the revenue-earning model of the trader. Additionally, the **Danish government** in their 2023 position paper considers the need for revising the definition of a transactional decision. The collective response from different Ministries in Denmark on this issue was that **protection from loss of autonomy should be at the heart of consumer protection**. They argued that:

“Retention mechanisms that influence consumers to spend excessive time on platforms, decrease the likelihood that consumers make a decision on whether to continue or discontinue to use the service should be covered by the UCPD”. An example cited mentioned earlier of such mechanisms include infinite scrolling and auto-play on social media.

The Danish government advocated in their position paper that retention mechanisms should be addressed in the UCPD by revising the scope of a “transactional decision” and the understanding of the “economic behaviour of the consumer” as defined in the guidelines to ensure clarity and to make the concept more operational for enforcement agencies. Because consumers (especially minors) may spend excessive time on platforms, infinite scrolling and auto-play on social media and similar mechanisms causing unwanted time-loss, the Danish government advocates that the UCPDs concept of a ‘transactional decision’ should be broadened to reflect all relevant consumer behaviour.

Whilst the study team recognises that time loss due to addictive design of social media platforms, some online games can be very problematic, and lead to various social problems (e.g. see case study on digital addiction, and the wide body of literature on the mental health effects of digital addiction on young people and wider social cohorts), there is a challenge as to whether regulatory or non-regulatory approaches are the optimal means of addressing the problem. For instance, major traders from global tech firms interviewed stressed that they take digital addiction as a problem very seriously and have introduced a variety of tools to tackle the issue, such as **time limits and parental controls** (tools available at the apps level but also at a systems / settings level via hardware). Regarding infinite scrolling, this issue is considered in more detail in the two EQs on problematic practices relating to digital addiction (see effectiveness and relevance). The main issue from a consumer protection perspective is whether voluntary industry-led measures such as time limits and parental controls are sufficient or not.

Conclusions – transactional decisions in the digital context

Despite the Commission’s broad interpretation of the concept of ‘transactional decision’ in the UCPD Guidance, there is an absence of case law applying the concept in a digital context, for example to attention-grabbing commercial practices in digital interfaces.

Stakeholder feedback (e.g. consumer associations, Ministries) showed that the concept of a transactional decision needs to be updated to ensure digital fairness. Due to the presence of digital asymmetries, the average consumer may - in certain circumstances - feel pressured into taking transactional decisions they would not otherwise have taken. A particular concern relates to minors being pressured into making transactional decisions online that could exploit their vulnerabilities, for instance in relation to impulse purchases and purchasing loot boxes whilst playing video games without checking the cost in real money terms. There is therefore a strong argument in favour of broadening the definitional scope of a transactional decision.

Regarding the attention economy, given that many digital services are provided for free and given the competitive nature of digital markets generally and of platforms in particular, some traders aim to maximise the time users spend on their platforms to optimise monetisation. Even though platforms may provide tools to monitor platform and/ or app usage, user interface design is often done in a way that could risk exacerbating digital addiction. Therefore, incentives should be created for industry to ensure that good practices in users having further control over their experience of using platforms

and apps and to control their design interface more easily could be effective. Examples are offering alternative layouts to infinite scrolling and the ability to opt out of autoplay.

Ensuring fairness by design and default from the outset would avoid bad practices in the over-manipulation of users' experiences, with a transition from passive to active consent. Nonetheless, as many digital services remain free, a balance needs to be struck. It should be recognised that creating an engaging in-app or in-platform experience is necessary to encourage users to be on their sites which is a fundamental part of traders' business models. Equally, there is a need to protect consumers from digital addiction to the extent possible, for instance by giving them opt-in and opt-out choices as to which functions they wish to enable/ disable. Requiring active rather than passive consent is another means of avoiding some of the most addictive elements (e.g. autoplay, which is not presently illegal, but which could be debated as to whether this practice could be considered as aggressive, given it consumes consumers' time without their active consent for suggested content).

EQ5 – How effective has the enforcement of the Directives been in relation to digital products, services and content?

Enforcement has long been regarded by many stakeholders as being one of the weak points in the implementation of the EU consumer law framework. The fact that in the public consultation and targeted consultation, a high share of consumers continues to experience problems in the digital environment points to a need to strengthen enforcement further. In previous studies, such as the 2017 fitness check of EU consumer law, coordinated enforcement of EU consumer protection rules was generally perceived to have improved over time thanks to the role of the CPC Network and the CPC Regulation applicable since 2006, shortly after the UCPD was adopted. The CPC Regulation was updated in 2017 and the revised rules came into force on 17 January 2020¹⁵².

Overall, enforcement remains a weaker aspect of legal implementation in EU consumer law, especially in the digital environment. A series of problems were identified that continue to undermine the effectiveness of consumer law in the digital environment, namely:

- Lack of proactive approach across the EU-27 towards taking on strategic deterrent cases in the digital environment (though some good practice examples in selected MS of taking on such cases in the digital environment (e.g. IT and NL).
- Absence of sufficient critical mass of national case law cases in applying the Directives in the digital environment for most problematic practices. Also, the considerable time taken for sufficient case law to emerge in the digital environment is problematic.
- The important role of regular sweeps by the CPC network in checking compliance with different aspects of the digital environment by traders, including most of the problematic practices identified in Section 4.2 should be stressed.
- The increased complexity of the EU consumer law framework, due partially to changes through the MD but mainly due to the increasing complexity and interconnectedness of different types of EU law and consumer law which must be applied by traders in parallel.
- Investigating potential infringements is therefore more complex, time-consuming, and resource-intensive explaining the comparative lack of legal cases.
- Progress however towards more harmonised approaches to penalties through the MD, which should have a dissuasive effect on traders in theory, but purported unevenness in penalties imposed by CPAs, raising a need for ongoing monitoring of how harmonised practices are among CPAs in issuing fines.
- The absence of any powers at EU level to issue fines to larger traders operating on a pan-

¹⁵² The Consumer Protection Cooperation (CPC) Regulation (EU 2017/2394) replaced the 2006 CPC Regulation (EU Regulation 2006/2004).

European basis to ensure consistency in fines (unlike the DSA).

It emerged from the interview programme that, in some jurisdictions, different public authorities may have overlapping competences with respect to consumer protection, such as authorities responsible for data protection, media, and electronic and digital communications. Interviews found that it can be challenging for CPAs to coordinate their work at national and cross-border levels across the diverse range of competent authorities in conducting investigations concerning digital products and services in the Member States. Feedback was received through interviews that there could be greater coordination and cooperation between CPAs and Data Protection Authorities (DPAs), given in the digital environment the increased interconnectedness between EU consumer law and the application of the GDPR and other data laws.

In addition to administrative enforcement, private enforcement i.e. through action by individual consumers or organisations is also foreseen in all Member States as civil claims can be by launched for infringing the directives. The toolbox of remedies is different according to the national provisions concerning contractual and non-contractual liability. According to national experts, private enforcement could be an effective instrument against breaches of the directives. Nevertheless, the level of protection granted to consumers varies according to the national rules of civil procedure, the length and costs of the proceedings and the extent to which alternative dispute resolution (ADR) mechanisms are easily available to consumers.

In collective redress cases, the Directive on representative actions for the protection of the collective interests of consumers 2020/1828 (the Representative Actions Directive), that replaced the Injunctions Directive 2009/22/EC¹⁵³, covers instances where traders infringe EU law that harm or may harm the collective interests of consumers, such as in general consumer law, but also in case of breaches of DSA, DMA, GDPR and other relevant digital instruments.

There is fragmentation and a diversity of solutions and actors, and the lack of coordination among them with respect to the goals of compensation and deterrence. Balancing these mechanisms is essential in terms of ensuring effective consumer protection with respect to digital products, services, and contents.¹⁵⁴

Legal cases undertaken by enforcement authorities involving digital aspects have been limited to date. The reasons underlying this were seen as including the following:

- **Complexity of applying the legal framework in the digital environment where often EU consumer law is being applied alongside digital and data law**, with infringements by traders potentially involving more than one piece of law in parallel. Digital asymmetries (informational and technological) mean it is complex to investigate if a particular practice is unfair to consumers (e.g. where there is decision-making bias in algo's that affects personalised pricing in a way that is unfair to cohorts of consumers). There is a need for **adequate technical expertise within CPAs** due to the complexity of taking on legal cases in the digital environment. Some CPAs have set up digital-focused divisions, such as within the Italian CPA and the Swedish Ombudsman but others have not and may lack capacity.

There have been several **high-profile legal cases** involving potential infringements of EU consumer law in the digital context, for example, including some taken on by the CPC network. When examining the existing body of case law and enforcement actions, it can be noted that there are legal cases that are cross-cutting in that they cover multiple Directives, pointing to

¹⁵³ We note that the Member States had until 25 December 2022 to adopt and publish measures to comply with the Collective Redress Directive and must apply these measures from 25 June 2023.

¹⁵⁴ Micklitz H.-W., Saumier G. (eds), *Enforcement and Effectiveness of Consumer Law: Ius Comparatum - Global Studies in Comparative Law*, Elgar, 2018.

the **increased complexity of applying consumer law in a digital context**. For instance, there are increasing interactions between data privacy issues under the GDPR and contract law under the UCTD and consumer protection rules around unfair and misleading practices under the UCPD. CPAs must invest in legal staff and sometimes in external lawyers to investigate increasingly complex cases, which are **resource-intensive and costly, necessitating selectivity in which strategic deterrent cases get taken on**.

Enforcers need to pursue complaints and/ or legal cases with non-compliant traders that have a demonstration effect. Some of these enforcement cases have considerable complexity given the interaction between different pieces of EU legislation. Concerning the **UCPD**, some CPAs mentioned that they are actively using the UCPD guidance to interpret how the law should be applied in a digital context. BEUC also mentioned that they have taken on strategic deterrent cases that sometimes cover more than one piece of legislation, such as the 2021-2022 CPC complaint against TikTok, which involved data protection concerns as well as various breaches of EU consumer law (UCPD, UCTD):

- Several terms in the 'Terms of Service' are unfair as they are unclear, ambiguous and favour the trader to the detriment of its users.
- The trader's 'Virtual Item Policy' which manages the popular feature that users can purchase coins which they use contains unfair terms and misleading practices. For instance, the right to modify the exchange rate between the coins and the gifts lies with the trader.
- The trader is alleged to inadequately protect children and teenagers from hidden advertising and potentially harmful content on its platform through videos showing suggestive content.
- The trader's practices for the processing of users' personal data are misleading as users are not clearly informed about what personal data is collected, for what purpose and for what legal reason.

Several Ministries and enforcement authorities interviewed referred to challenges regarding the **length of negotiation and/ or redress procedures** for online actors to come into compliance. In the case of global traders, some interviewees perceived that despite the recent improvements introduced under the MD to strengthen the harmonisation of penalties within the EU-27, there has been a limited deterrent effect of the associated sanctions. This was mentioned in relation to the enforcement of all consumer law Directives.

Regarding **stakeholder feedback on the effectiveness of enforcement activities**, a 2023 survey by BEUC and national consumer associations found that respondents were generally unhappy with the level of consumer protection provided by consumer protection authorities (CPAs). The dissatisfaction level was highest in Romania (46%) and France (40%) and lowest in Sweden (26%) and Italy (28%).

The issue of the comparatively low number of legal cases pertaining to the application of EU consumer law in the digital environment makes enforcement more challenging for CPAs as they have only limited case law to rely upon when considering undertaking enforcement actions. A related issue raised was the time lag between the identification of problematic practices considered to be potentially unfair, misleading, deceptive or aggressive; and relevant case law emerging in relation to new business practices which creates a bottleneck in terms of the lead times needed before enforcement can be strengthened.

This was raised for instance in the targeted survey and in some position papers. VBVZ noted that the development of relevant case law of the CJEU noted the difficulties in obtaining timely improvements in the application of EU consumer law through reliance on case law. "Consumer

rights-friendly CJEU rulings play a paramount role in the interpretation and enforcement of consumer law. However, obtaining them takes time and can only be achieved selectively".

Legal academics authoring the ELI contribution to the fitness check mentioned the drawback of relying on the general principles-based approach presently without more specific regulatory requirements for some specific digital practices. It was noted it can take years for legal clarity to emerge through case law in relation to a particular emerging digital business practices. By the time that legal certainty is provided, there may be many new digital practices and business models creating fresh uncertainty.

The country analysis also points out that **cross-border cases of infringement of the Directives are particularly complex and problematic**. Some countries have more robust enforcement agencies and systems in place, while others may lack resources or expertise in dealing with cross-border consumer disputes effectively. These disparities can complicate cross-border cases and hinder the consistent protection of consumers' rights throughout the EU.

A further issue in respect of cross-border cases for enforcement is whether there are sufficiently common penalties. This issue is explored in detail in relation to the impact that changes to strengthen the harmonisation of penalties have had since the Modernisation Directive came into application in May 2022. However, some stakeholder feedback was received that there continues to be a problem with divergence in the level of penalties between MS, although it is too early to assess the full impact of the MD, which has fostered greater harmonisation in penalties in legal texts. Feedback was received that enforcement practices vary at national level across the EU-27 and the level of penalties varies widely, with many legal cases being undertaken at national level and relatively few being cross-border.

This raises an issue as to whether the CPC Regulation should be strengthened in the future such as to allow the European Commission a new role in enforcement of cross-border cases rather than solely relying on national CPAs given the significant transnational dimension of some of the cases concerned and the size of the traders concerned, who have more resources at their disposal than national CPAs, whose resources vary considerably and are limited by national budgets.

According to national authorities and ministries, the interplay of the UCTD, UCPD and CRD with the **Digital Services Act (DSA)** in terms of enforcement, including about specific issues such as transparency in online marketplaces, remains unclear to date. Thus, there is a high level of legal uncertainty among authorities, practitioners and officers in the Member States in this respect.¹⁵⁵ A key issue raised was that the European Commission has been given new enforcement powers under the DSA to take enforcement actions against platforms in cases of infringements. Given the cross-border dimension of digital services and markets, this raises the issue as to whether the enforcement of EU consumer law can be sufficiently effective given the global nature of many traders in these markets without a more common, EU-wide approach to enforcement, possibly with a role for the Commission, but only in larger cases.

Based on interview feedback and a review of public consultation and targeted consultation position papers, there was common agreement as to the important role of enforcement in ensuring uniform levels of consumer protection and a level playing field for traders. However, there were differences in perception as to how effective enforcement has been overall to date. The targeted survey identified positive perceptions of the effectiveness of enforcement possibilities for EU consumer law in the digital environment. Consumer redress, the resolution of dispute between consumers and traders through out-of-court dispute resolution mechanisms and the private enforcement by qualified entities were the most effective enforcement tools/strategies with respectively 69.0%, 65.7% and 65.7% of respondents

¹⁵⁵ Wilman, F. (2022). The Digital Services Act (DSA) - An Overview, dx.doi.org/10.2139/ssrn.4304586

claiming them to be either very effective or effective. At the second and third digital consumer summits held in November 2022 and November 2023 respectively, and in some interviews, especially consumer and trade associations, but also Ministries, advocated for strengthened and more uniform enforcement of EU consumer laws. However, a challenge in this regard is that enforcement also depends on national procedural rules for CPAs and for the courts.

Some stakeholders (e.g. traders, trader associations) pointed to **the lack of uniform interpretation of EU consumer law by CPAs** as a challenge. This was attributed as being due to various reasons, such as the transposition process leading to different interpretations of the rules in different Member States. In addition, there are different interpretations according to some stakeholders regarding what is definitely prohibited, especially for practices where there may be grey areas regarding certain commercial practices, such as personalised advertising. For instance, whereas it is not permissible to target minors with direct exhortations under either the UCPD or with targeted advertising under the DSA, it is ambiguous which types of personal data can be used to personalise advertising under the UCPD. For instance, the DSA prohibits targeted advertising on the grounds of sensitive data, only by online platforms, but there is no such precision regarding which personal data can and cannot be legitimately used under the UCPD.

Some CPAs interviewed acknowledged that there are a small number of CPAs (e.g. in Italy, the Netherlands) that have been **proactive in taking on strategic deterrent cases against traders** to test their regulatory enforcement powers within the limits of the existing legal framework. CPAs have different limitations and motivations and their level of activity depends on their human and financial resources. A CPA cannot be proactive if it is not well-funded and organised. Regarding the structuring of enforcement activities, it can be observed that experience from outside the EU-27 may be relevant. For instance, in the UK, the national CPA has established a digital unit to tackle problematic practices in the digital environment. Even if legislation is technology-neutral and treats online and offline equally in parallel, there may be specific and technically-complex issues (e.g. fairness of AI systems and algo's, scalper bots) that require specific expertise and technical competences to be developed. The possibility of CPAs setting up digital units to specialise could be considered as a possible recommendation.

However, other good practices of public enforcement can be highlighted. Whilst the Commission has published guidance on all three Directives and some CPAs have published national guidance. For instance, the Netherlands Authority for Consumers & Markets (ACM) has published guidelines on the protection of online consumers. These also reflect the interaction between EU consumer law and other EU legislation, such as evolving privacy laws and the data privacy landscape. A further good practice from the Netherlands is **joint cooperation between different enforcement authorities**.¹⁵⁶ For instance, the Dutch Data Protection Authority (AP), the Netherlands Authority for Consumers and Markets (ACM), the Dutch Authority for the Financial Markets (AFM), and the Dutch Media Authority (CvdM) will work together to strengthen oversight of digital and online activities through the launch of the **Digital Regulation Cooperation Platform (SDT)**.

Participating regulators will exchange knowledge and experiences gained from their day-to-day oversight activities in areas such as artificial intelligence, algorithms, data processing, online design, personalization, manipulation, and misleading practices. They will make joint investments and share / develop knowledge, expertise and skills. They will explore where they are able to strengthen each other's work in enforcement procedures, for example, by dealing with digital market problems collectively.

¹⁵⁶ <https://autoriteitpersoonsgegevens.nl/en/news/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation>

Some feedback on means of strengthening enforcement in respect of specific Directives was also received. For instance, the UCTD case study found there to be a need to strengthen the enforcement side of the UCTD, both on the preventive front (e.g. more awareness-raising and guidance, or exploring the possibility of dialogue and negotiation with global traders) and by increasing deterrent effects, including through CPC network and joint actions, and especially towards global traders with significant market powers.

Many trader associations mentioned the importance of using existing enforcement powers to the full, in combination with effective guidance, to improve the effective working of the existing regulatory framework before making any further changes to the EU consumer law framework. Most categories of stakeholders highlighted scope for additional EU and national work on (1) enforcement, and (2) by increasing deterrent effects, including through CPC network joint action, especially towards mass market actors that hold huge power on global markets (more so where competition and alternative online service or product providers are limited).

However, for consumer associations and some Ministries, CPAs and legal academics, there may be a need for more specific rules in a few problematic areas to clarify the legal framework. This could help to improve enforcement. For instance, an interviewee from a Ministry pointed out that they would like to have specific rules in certain areas such as issues around which types of personal data can legitimately be used by traders in personalised advertising and pricing and which cannot, and a cancellation button to allow customers to exit from subscriptions (including subscription traps) more easily. This would make it easier for CPAs to determine whether traders are compliant or non-compliant, which presently is more difficult and requires timely and costly investigation. However, other stakeholders, especially trader associations and individual traders cautioned that as EU consumer law is implemented through Directives, with some regulatory divergence in interpretation, introducing further rules could lead to additional fragmentation, which in turn could make enforcement activities more complex. As the body of EU consumer law in combination with other applicable law has evolved due to the gradual accretion of different rules, and further regulatory amendments made to the underlying legislation through the Modernisation Directive, it was argued that this can make legal interpretation more complex for CPAs.

Consumer law is already fragmented, given that in addition to core applicable EU legislation under the UCPD and UCTD, plus the CRD, there is sectoral legislation covering consumer protection in the digital environment. However, there is also an issue regarding the interplay with other legal norms, e.g. e-commerce (plus the DSA and the DMA), data protection legislation e.g. the GDPR, e-Privacy Directive and new legislation on data sharing, the Data Act, to mention a few. There are therefore two different levels of challenges for CPAs to navigate when undertaking enforcement activities: a) the fragmentation of consumer law and b) overlapping legal norms with consumer law (e.g. the GDPR and e-PD) given the increasingly interconnectedness of the legislation in the data-driven internet era. This has also been recognised in academic literature¹⁵⁷.

Coordination and cooperation between CPAs and other types of enforcement authorities

A further point may concern the open issue of ensuring **more effective coordination of CPAs and Data Protection Authorities (DPAs)** in cases involving consumer protection with a data protection dimension. Given that these different types of legislation are overseen by different types of enforcement authorities, there is an issue around the lack of cooperation between the two, which has been noted in previous studies. It is important to mention, however, that the CPCs and DPAs have a joint collaboration group, which in 2022 published a joint

¹⁵⁷ Graef, Inge ed others (2018), Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law, International Data Privacy Law 8(3), p. 200-223, Available at SSRN: <https://ssrn.com/abstract=3216198>

recommendation on principles to follow when marketing advertise to children.¹⁵⁸ However, looking ahead, this could become an increasing challenge given data is crucial to the digital economy and DSM. The difficulty in bringing together coordinated enforcement of consumer protection laws across a raft of new digital legislation, including sectoral legislation on digital services and markets, with data-driven legislation is recognised by CPAs and has been highlighted *inter alia*, by BEUC in its position paper on the CPC Regulation revision¹⁵⁹.

The potentially relevant role of **equality bodies** should also be mentioned in the context of **equal access to, and supply of goods and services**. National equality bodies were set up under EU equality laws. A new proposal for a Directive on standards for equality bodies was issued by the Commission in 2022.¹⁶⁰ The work of CPAs should therefore consideration equality-related considerations insofar as these may impact the achievement of high levels of consumer protection.

Looking ahead, some stakeholders (e.g. CPAs, trader associations) commented that there are likely to remain challenges in improving the effectiveness of enforcement, such as constraints in human and financial resources available for enforcement at national level. Some large traders and trader associations would also like CPAs to be more proactive in taking action against non-compliant traders to ensure that their investments in regulatory compliance are not wasted.

A further example raised by some stakeholders (e.g. consumer associations, legal academics) of a mechanism to improve compliance and make it easier for enforcers to check compliance is the possibility of introducing a **digital fairness by design requirement** to the UCPD and UTCD applicable from the outset of website and app design, such as to prevent problems such as dark patterns; or in the case of contract terms, difficulties locating terms of the contract, or “click and browse wrap” presentation of terms¹⁶¹. This concept is analogous to the GDPR’s Article 25 (Data protection by design and by default)¹⁶² and the DSA’s provisions that regulate interface design (e.g. Article 32 on compliance by design). Such concepts could also facilitate consumer law enforcement, for example by making it clearer in the UCPD that interface design should be fair. Some stakeholders (e.g. consumer associations, some legal academics) believe such concepts should be extended to the UCPD. Commenting on the topic of fair design, the **Netherlands Authority for Consumers and Markets** outlined in a position paper (public consultation response) that *“commercial digital environments should be fair to consumers. They should not contain design choices or techniques that harm consumers, whether that is financially, emotionally, in terms of time lost, privacy lost or by creating addiction. Whether a digital environment is fair to consumers should be tested”*.

A possible gap was however identified in relation **to ensuring more harmonised penalties across the EU**. Whilst the sanctions regime has been harmonised *to an extent* through the Modernisation Directive in theory, with common maximum penalties, only for infringements subject to coordinated enforcement action under the CPC Regulation, now more aligned with the turnover-based fines in other EU legislation such as the GDPR, in practice, different Member States have differing traditions in terms of issuing sanctions in respect of civil law infringements. Whereas some hardly issue fines at all, others have issued punitive fines aimed at ensuring an effective deterrent. This ongoing divergence, despite the best efforts of the MD

¹⁵⁸ https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cooperation-between-consumer-and-data-protection-authorities_en

¹⁵⁹ STRENGTHENING THE COORDINATED ENFORCEMENT OF CONSUMER PROTECTION RULES (2022), BEUC Position Paper - https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-135-Strengthening_the_coordinated_enforcement_of_consumer_protection_rules.pdf

¹⁶⁰ Proposal for a Council Directive on standards for equality bodies in the field of equal treatment between persons in matters of social security and in the access to and supply of goods and services, 8th December, 2022 - https://commission.europa.eu/document/download/797a4729-bc57-4e91-b703-bb4bdea8b4_en

¹⁶¹ Whereby ‘access a webpage’ or ‘signing-up’ equates to agreeing to contract terms.

¹⁶² <https://gdpr-info.eu/art-25-gdpr/>

to strengthen the harmonisation of sanctions, means that the role of penalties in supporting pan-European enforcement is undermined.

It was mentioned in interviews that some major cases involving traders have resulted in very disparate fines for breaches of EU consumer and other types of legislation, which may be very low in some MS, and running into the millions of EUR in others, undermining the effectiveness of the penalties regime, despite the positive changes made to strengthen the harmonisation of penalties through the Modernisation Directive (where it is too premature to assess the full impact, given that the regulatory amendments to harmonise penalties have only just come into force).

This raises a strategic question as to whether EU bodies have sufficient enforcement powers in consumer law and whether they should play a stronger role in enforcement and the issuance of penalties when cases involve non-compliance in multiple markets, with pan-European relevance.

The **possible revision of the CPC Regulation**¹⁶³ could provide an opportunity to strengthen enforcement, for instance through expanding regulatory enforcement powers in relation to EU-wide infringements. Some stakeholders interviewed e.g. for the UCTD case study, among others, suggested that the amending of the CPC Regulation could be an opportunity for CPAs to invest in positive or soft enforcement, such as entering into dialogue and negotiations with global traders and awareness-raising on existing requirements amongst small traders, rather than focusing on sanctions and hard enforcement such as court action, lengthy by nature and therefore not adapted to the speed of change in the fast-paced digital environment. An interviewee from the Commission working with the CPC Regulation mentioned that there are many awareness-raising activities as well as efforts by the regulator to reach out and work with major e-commerce players and marketplaces and platforms to resolve problematic issues and / or to discuss and rectify non-compliance by traders.

CPAs are becoming **increasingly familiar with the use of "sweeps" - coordinated monitoring activities to detect unfair practices online**. These sweeps play an important role in allowing CPAs to systematically scan websites and online marketplaces for potential consumer rights violations, such as misleading advertising, unfair terms, or non-compliance with disclosure obligations. By employing such collaborative enforcement tactics, CPAs aim to enhance the detection and deterrence of unlawful practices across digital platforms. The approach is particularly effective in the digital context where e-commerce activities span multiple jurisdictions, making the traditional, isolated enforcement efforts less effective. For example, the Authority for Consumers and Markets in the Netherlands have built a tool in-house which can scan many hundreds of websites to see which contain countdown timers, which can then be checked by staff to see if they break misleading price rules¹⁶⁴.

Finally, it is worth considering how far there are any **examples of good practices by traders** and their representative associations in tackling problematic practices. It is in the interest of both traders and consumers that traders also play their role in applying and disseminating good business practices to a wider range of traders such as to strengthen the level playing field and to improve consumer protection. Collectively, these various tools – guidelines, codes of conduct, tools to monitor app or phone usage, parental control tools help to strengthen consumer protection and, in some cases, tools for disclosures regarding paid promotion or sponsorship which make it easier for traders to comply with the law. It should be noted that the role of Commission's legislative guidance in tackling problematic practices was strongly highlighted by many stakeholders interviewed.

¹⁶³ See Consumer protection – strengthened enforcement cooperation, Call for evidence for an Impact Assessment, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13535-Consumer-protection-strengthened-enforcement-cooperation_en

¹⁶⁴ <https://www.acm.nl/en/publications/acm-confronts-online-stores-using-misleading-countdown-timers-their-practices>

3.1.3.1 Good practices among traders and their associations

Good practices among traders and their associations in strengthening digital fairness and compliance with EU consumer law in the digital environment were identified through interviews and desk research. Whilst recognising that some traders are bad actors and part of the problem, good faith traders should be recognised as being part of the solution.

Whilst the research has identified evidence of negligent or intentional non-compliance among traders in some areas, there are also good faith actors that can play a positive role in increasing compliance and in disseminating good practice regarding how to comply effectively with EU consumer law and where regulation of specific practices is not explicit, in taking preventative measures. There have been some voluntary initiatives by traders and/ or their representative associations to strengthen consumer protection. These are worth noting when considering how best to address problematic practices in future (also see possible solutions to such practices under 'relevance'). Examples include joint policy-maker / trader initiatives (e.g. the Cookie Pledge initiative and "Digital Consumer Rights Commitments" in the Consumer Protection Pledge in which many global tech players are participating and industry-led voluntary initiatives in areas such as video games and age-appropriate ratings) and user-oriented tools provided by traders that help consumers to manage online experiences as a means of addressing some problematic practices. There is scope to transfer good practices to SMEs from larger players such as online platforms and marketplaces, e.g. in compliance with information disclosure requirements.

Concerning **subscriptions**, some traders remind customers about subscriptions after a certain period, such as prior to the renewal of an annual subscription. In addition, more recently, major credit card companies have also begun to inform consumers by email and/ or SMS if a subscription renewal is due (presumably, to avoid a situation where many consumers complain which would be resource-intensive). Whilst this represents good practice, not all traders provide such reminders.

Concerning the risk of **hidden advertising by influencers**, major platforms such as YouTube have developed easy to use tools such that content creators can when uploading their content make it clear if the video contains a paid promotion or sponsorship. Whilst disclosures are required under EU law¹⁶⁵ (e.g. the e-commerce Directive, the AVMSD), the ease of use of these tools to label videos appropriately can be considered a good practice. Furthermore, regulatory and industry guidance was found to play a role in several Member States, such as in some of the Nordic countries and the Netherlands. At EU level, EASA updated in 2015 its Best Practice Recommendations (BPR) on Digital Marketing Communications (DMC) which extended the scope of advertising self-regulation to all forms of marketing communications, including influencer marketing.¹⁶⁶ In 2023, the EU has also funded an Influencer Legal Hub to educate content creators and industry professionals.¹⁶⁷

Furthermore, concerning transparency measures by large platforms regarding **online advertising** more broadly, Meta notes in its response that they provide users with tools so they understand how their data is used. Tools include "Off Facebook activity" - a summary of information about data other apps and websites have sent to Meta, which allows people to disconnect this information from their account, and the "why am I seeing this ad?". Meta has made a recent update to link from "why am I seeing it" to privacy and ad settings which can be amended. It is possible to disconnect third party apps, and not to see content from a given advertiser.

¹⁶⁵ Directive 2000/31/EC on Electronic Commerce (Art. 6) requires influencers to mention commercial partnership and the company for which this communication is made, while the Audiovisual Media Services Directive (AVMSD) requires audiovisual commercial communications on e.g. video-sharing platforms to be readily recognizable as such. These information and transparency obligations are applicable across the EU.

¹⁶⁶ <https://www.easa-alliance.org/issues/influencer-marketing/>

¹⁶⁷ https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/influencer-legal-hub_en

Concerning **digital addiction**, several online platforms have developed a range of tools for users to monitor their usage and for children and minors, a range of parental control tools to tackle problems such as social media addiction. There are many different monitoring tools to check time spent at the device level and in-app and on platforms. Concerning **video games** specifically, there are industry-led initiatives by producers of games consoles to provide parental controls to enable control of the time spent on video games by minors and children. There are also efforts by many game developers to enable parents to set spending limits and/ or to prevent in-game (and / or in-app spending) for minors (e.g. on loot boxes).

Furthermore, there are initiatives for providing more **age-appropriate pre-contractual information on video games**. PEGI is a well-known age-appropriate labelling system¹⁶⁸ which takes the form of a Code of Conduct and “provides parents and consumers with objective, intelligible and reliable information regarding the suitability of a game’s content, prior to purchase, or prior to engaging with a game. A label is assigned to the game (i.e., PEGI 3, PEGI 7, PEGI 12, PEGI 16, or PEGI 18). The aim is to enable consumers to make informed choices about video games they would like to play or to buy, by displaying the appropriate age for playing the game and the type of content featured in the game, e.g. violent content, bad language, etc. The rating criteria provide for a framework against which the age-appropriateness of certain types of content or gameplay activities is assessed. The level of awareness of the PEGI age labels is high, 75% label. The PEGI system was designed by the industry itself to protect minors and behave responsibly, especially concerning children. Concerning loot boxes, 11 industry principles were developed jointly between Ukie, the industry body and national regulators in the UK¹⁶⁹. The guidance is explored in more detail under the digital addiction topic, which also covers loot boxes.

Age-appropriate design codes could be a means of mitigating some of the problems that children face as vulnerable consumers, such as digital addiction or preventing children and minors from accessing material which is not suitable for their age group. In an interview with a children and minors' rights organisation focusing on digital matters, it was suggested that the optimal way forward would be to strengthen the definition of a vulnerable consumer to include children, at least in the recitals to support Art. 5(3) UCPD, but not to seek an outright ban on children using particular services, unless justified. For instance, the organisation concerned was not against age-gating of certain websites or apps from children (e.g. porn sites).

However, the national law in FR which prohibits access to social media platforms for under-15s was not viewed as being effective necessarily, as it could be circumvented. Therefore, they advocated an in-between approach which would strike the right balance between protecting children and minors whilst not preventing their access to age-appropriate services, and instead building in age-appropriate design from the outset. In this regard, the development of age-appropriate design codes has become more common as a tool to ensure that design interfaces consider the specific and rights of children and minors. However, there are variations in terms of whether a regulatory or non-regulatory approach has been adopted. For instance, in the US and UK, a regulatory approach was chosen e.g. in California, through the California Age-Appropriate Design Code Act in 2021-2022.¹⁷⁰

At EU level, a special group has been formed by the Commission’s DG CNECT on the **EU Code of conduct on age-appropriate design**.¹⁷¹ This was identified as a key action under the European strategy for a better internet for kids (BIK+). The strategy was adopted on 11 May 2022, and will ensure that children are protected, respected and empowered online in the new Digital Decade, in line with the **European Digital Principles**. The BIK+ strategy

¹⁶⁸ <https://pegi.info/what-do-the-labels-mean>

¹⁶⁹ New Principles and Guidance on Paid Loot Boxes - <https://ukie.org.uk/loot-boxes> and <https://www.gov.uk/guidance/loot-boxes-in-video-games-update-on-improvements-to-industry-led-protections>

¹⁷⁰ https://leginfo.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

¹⁷¹ <https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids>

incorporates a number of key pillars that are relevant to this study in that achieving digital fairness for all EU consumers implies a need for particular attention to more vulnerable groups. There are also safeguarding issues in terms of protecting children in the digital environment. For instance, whilst dating platforms typically have a minimum age requirement of 18+, this commonly is enforced by asking people to tick a box to confirm that they are 18 or older, which is a “self-declaration”. However, this is not an effective approach. The use of AI technologies in age verification also has shortcomings due to low accuracy.

Beyond the development of an EU code, a number of EU countries have already adopted national guidelines and codes:

Ireland (2021) - the Irish Data Protection Commission (“DPC”) published guidance “Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing” (“the Fundamentals”).¹⁷²

The Netherlands (2021) - a code for children’s rights published by the Ministry of the Interior and Kingdom Relations¹⁷³ based on 10 principles: Principle 1: Make the best interests of the child the primary consideration when designing. Principle 2: Involve children and their expectations in the design process. Principle 3: Ensure the legitimate processing of personal data of children. Principle 4: Provide transparency in a way that is understandable and accessible to children. Principle 5: Carry out a privacy impact assessment based on children’s rights. Principle 6: Provide a child-friendly privacy design. Principle 7: Prevent the profiling of children. Principle 8: Avoid the economic exploitation of children at all times. Principle 9: Avoid a harmful design for children at all times. Principle 10: Develop industry guidelines which are geared to protecting the interests and rights of children.

Sweden (2020) - the Swedish data protection authority ('Datainspektionen') published guidance to strengthen children's and young people's rights online. In particular, the Datainspektionen noted that this year the Convention on the Rights of the Child became law in Sweden, and to strengthen children's rights online, it had jointly produced with the Children's Ombudsman and the Swedish Media Council a guide for actors responsible for social media, games and other digital environments.¹⁷⁴

In the area of standardisation, CEN-CENELEC are working on the development of a new standard which will provide a framework for developing age-appropriate digital services for situations where users are children as to how to design digital services for children.¹⁷⁵

3.2 Efficiency

According to the ‘Better Regulation Guidelines’, evaluations should examine the costs and benefits of the EU intervention as accrued to different stakeholders, identifying the driving factors, and how these relate to the EU intervention. The analysis considers the ratio between benefits and costs in respect of EU consumer legislation and the achievement of digital fairness. The analysis of efficiency considers the cost drivers of compliance for traders, the administrative burdens for enforcement authorities and the costs for consumers of any evidence of legal gaps (from a consumer detriment perspective). The extent to which there has been any simplification of EU consumer law and its application is also considered.

The following sections aim to answer the following questions:

EQ6 – What are the regulatory compliance costs (administrative, adjustment costs) of the

¹⁷² Fundamentals for a Child-Oriented Approach to Data Processing – Irish DPC - https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

¹⁷³ https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf

¹⁷⁴ <https://www.dataguidance.com/news/sweden-datainspektionen-publishes-guidance-childrens>

¹⁷⁵ <https://www.cencenelec.eu/news-and-events/news/2022/workshop/2022-03-28-digital-services/>

Directives for the different actors involved (Member States authorities, businesses, consumers) and for consumers overall in the digital area?

EQ6(1) – What is the cost for businesses to comply with the Directives, including specifically for SMEs considering different kinds of SMEs operating in the digital sector(s) by size threshold (micro, small and medium firms)?

EQ6(2) – What is the cost of compliance with the Directives for SMEs? Is it possible to observe any differences between different kinds of SMEs operating in the digital sector(s) (e.g. micro, small, and medium)?

EQ6(3) – Are there any benefits of practices in the digital environment that may partially offset consumer detriment?

EQ6(4) – What are the main benefits of consumer law Directives in theory? How far have these actually been manifested in practice?

EQ6(5) – 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 the society?

EQ6(6) – Are there opportunities to simplify the legislation or reduce unnecessary regulatory costs without undermining the intended objectives of the Directives?

EQ7 - What are the benefits of EU consumer law in terms of ensuring digital fairness and wider benefits?

3.2.1 Overview of the methodology and summary of the results

Whereas consumer laws have traditionally been applied by e-commerce firms, traders active in the market have diversified, given developments in digital markets, and include online marketplaces, platforms and new types of traders, such as (professional) social media influencers and other content creators.

The main steps in estimating the costs to traders have involved the following:

- Step 1 – collection of secondary data on market size and structure (no. of enterprises, turnover) to develop an overview of digital markets and services.
- Step 2 – primary data collection to gather data on the costs and benefits of EU consumer law, the frequency of problems encountered in the digital environment and incidence of consumer detriment.
- Step 3 – development, testing and validation of assumptions (e.g. regarding the average and median costs of compliance with EU consumer law in digital environment, % of consumers that experience problems who also experience detriment).
- Step 4 – extrapolation of costs and benefits to the EU-27 level;
- Step 5 – consideration of any data limitations in the estimates.

The approach to estimating the costs and benefits to consumers is based on the concept of consumer detriment.

The following table summarises the main sources of data for the different parts of the efficiency section and related justifications. The detailed methodology for assessing costs and benefits is summarised in Annex 7, including the main assumptions, and any caveats with the interpretation of findings.

Table 3-2 – Overview of sources of data for assessing efficiency

Stakeholder	Main source of data	Other data sources	Additional notes	Data limitations
Traders	Primary: Enterprise survey	Primary: Targeted consultation Primary: public consultation Interview feedback Secondary data (e.g. Eurostat and trader association data on market size and structure of European e-commerce sector, platform and subscription economies).	Sample size of the enterprise survey larger than targeted consultation to aggregate costs across the EU. Other data sources have been used for validation and further insights into type of costs (e.g. targeted survey, interview feedback). The public consultation provides general views on benefits to traders. Secondary statistical data provides context e.g. shows the evolution in market size and structure, trends and developments (see Section 3.2.2) across key areas of the digital economy.	Eurostat data does not cover the digital economy well, given that NACE codes are not well-aligned with the rapid development of e-commerce and wider digital markets and services.
Consumers	Primary: Consumer Survey	Primary: public consultation Secondary data	Consumer survey included a survey of 10,000 consumers. Consumer survey included questions about financial consumer detriment.	Absence of EU-wide data on volume of complaints made by consumers (for development of assumptions regarding consumer detriment).

The costs of compliance with the Directives were analysed drawing on the limited quantitative costs data provided by traders and their representative associations through the enterprise survey (and where questions were included, also from the targeted and public consultations), complemented by a review of previous evaluations and other studies to obtain any benchmark data. Some data on non-compliance was also obtained based on survey feedback and the results from CPC sweeps and the sweeps undertaken in this study. Some qualitative feedback on compliance costs was obtained through the targeted and enterprise survey undertaken as part of this study.

A few observations regarding the types of costs data that it was possible to obtain and what was not feasible to quantify are summarised below. The methodological annex on the CBA approach provides further technical detail (see Annex 7):

- Whilst the analysis has considered **both one-off and recurring compliance costs**, it is important to note in relation to one-off costs that these are relatively modest, firstly as the Directives were adopted in 1993, 2005 and 2011 respectively, for many companies these costs were incurred years ago. Therefore, compliance costs estimates mainly focus on recurring costs estimates.
- Secondly, the one-off costs would **not have been specific to digital fairness**, but related to complying with consumer law more generally. Disentangling compliance with EU consumer law requirements in the digital environment compared with offline compliance was not easily possible, given the lack of digital-specific requirements until

the MD was adopted (and even then, very few), and the technology-neutral design of the legal framework.

- However, an effort was made to capture some of the more recent **one-off costs associated with new information requirements** due to the Modernisation Directive's transposition and the amending effects on the underlying consumer laws. Information costs for the core Directives pre-MD are not applicable as traders only need to comply with the general principles and ensure they meet the general fairness test and not under reporting or information obligations (except for MD-related transparency requirements for platforms which are new).
- Some **adjustment costs** were estimated due to familiarisation with EU consumer law requirements and their application in the digital environment. Further examples of such costs include having to redesign processes or websites were envisaged from existing retailers operating in digital platforms and affected by the new information disclosure rules introduced by the MD in 2022. The largest costs mentioned in consultation include the costs of providing information on ranking criteria, processing of reviews, communication and price discounts (in decreasing order). These adjustment costs include the costs of new software acquisition, a one-off investment. Software development costs in Europe vary widely depending on the geographic location. For instance, in Western Europe and in Scandinavian countries, estimates are between 90 - 140 EUR per hour, whereas in central and Eastern Europe from EUR 23 to EUR 45 per hour, excluding taxes and fees but companies are likely to outsource IT services to minimise costs.¹⁷⁶ The costs of hiring external services have been estimated in consultation to be EUR 1,600 (median); equivalent to three days of an IT expert's time. In 2022, 22.9% of EU enterprises conducted online sales using websites or apps; but according to the consultation, only 10% of companies experienced at least some adjustment costs. **The adjustment costs can be estimated to range between EUR 208-303 million annually.**
- Companies, including SMEs navigating software costs and consumer protection regulations, must stay informed and adapt to the evolving digital landscape and check their compliance (also to avoid a maximum fine of at least 4% of the seller's turnover for non-compliance). These are the largest costs recognized by companies and they are recurrent. They could include software maintenance, direct labour costs, or the cost of external services related to compliance. These costs were estimated in consultation to be EUR 1,800, as the median value, for the lower range, and EUR 2,500 for the upper, which includes external services, and 15% of the companies reported this type of costs. **The administrative costs can be estimated to range between EUR 249.8-487.5 million annually.**
- **Other recurring administrative costs** from e.g. reporting and/or other administrative obligations on traders are expected to represent a **negligible** part of compliance costs, since the directives do not establish any reporting requirements.

3.2.2 Evolution in B2C digital markets and services and review of market size

This section sets out key developments in the evolution of digital markets and services focusing on the period from 2016-17 when the previous fitness check was performed to 2023-24 when the current fitness check was conducted. However, the previous study only partially addressed either problematic practices or the digital environment. Nonetheless, as per the Better Regulation Guidelines (BRG), it is important to assess the problem's size and to consider how far the problematic practices analysed in Section 2 have led to consumer

¹⁷⁶ <https://ncube.com/the-cost-of-it-services-in-europe>

detriment from a digital fairness perspective.

The analysis begins by providing a description of key digital markets and services within the European Digital Single Market, which also contextualises Europe’s competitive position internationally. The baseline situation and how far a comparison can be made to assess progression in terms of digital fairness is then provided.

The following summary box provides an overview of the baseline and current situation across some of the key B2C digital markets and services. The size of the European market is mentioned where available, and alternatively, any estimates of global market size.

Table 3-3 - Overview of European market size by area of B2C digital markets and services

Digital markets and services	Original baseline in 2016-17 (where available)*	Baseline situation in 2023-24*
Ecommerce	European e-commerce sector had major growth in 2016 and 2017. In 2016, the B2C e-commerce turnover in Europe was approximately €530 billion (15% increase compared to the previous year). By 2017, the sector's turnover was forecasted to reach around €602 billion, (14% growth). ^{177, 178}	In 2023, the B2C e-commerce turnover in Europe was estimated at €990 billion, marking a continued expansion despite economic challenges. This growth trajectory reflects an increase from previous years, with the turnover being €899 billion in 2022 and €849 billion in 2021. ¹⁷⁹ A more conservative estimate is that revenue in the European eCommerce Market projected to be €582.7 billion in 2024. ¹⁸⁰ The market value expected to increase from €610.7 million (2023) to €1202.1 million (2027). eCommerce report 2023, Statista, January 2023. ¹⁸¹
Digital advertising	European digital advertising market experienced significant growth in 2016-17. In 2016, market size was approximately €41.9 billion. By 2017, it had grown to around €48 billion, a 14.4% increase. Growth was driven by search and display, video advertising, social media and mobile ad expenditure. ¹⁸²	European digital advertising market reached an estimated €86 billion (2022) (IAB Europe, Statista), having grown by expand by 9.8% in 2022, down from 31% growth (2021). Future CAGR (compound annual growth) projected to be 6.87% (2024-2028) with global turnover of US\$96.6bn by 2028. ¹⁸³
EU platform economy	EU's platform economy has grown exponentially from an estimated €3 billion in 2016 to €14 billion in annual revenues by 2020. ¹⁸⁴	Assumption - growth continued at similar pace in 2021-24 period. Estimated by CSES that with a growth rate of approximately 8-10% per annum, figure may have increased to €19 billion (2024).
Subscription economy	In 2016-17, the subscription economy in Europe expanded rapidly, with subscription businesses growing at a rate of around 22% annually by 2017.	Telecoming estimated that in 2021, 560 million subscriptions were purchased by EU consumers (25% of the worldwide total). ¹⁸⁶

¹⁷⁷ <https://ecommerce-europe.eu/press-item/european-ecommerce-report-2017-released-ecommerce-continues-prosper-europe-markets-grow-different-speeds/>

¹⁷⁸ The e-commerce Market in the European Union, Enterprise Europe Network - https://een.ec.europa.eu/sites/default/files/een_guide_ecommerce_2018.pdf#:~:text=URL%3A%20https%3A%2F%2Fecn.ec.europa.eu%2Fsites%2Fdefault%2Ffiles%2Fecn_guide_ecommerce_2018.pdf%0AVisible%3A%200%25%20

¹⁷⁹ European e-commerce report - <https://www.eurocommerce.eu/european-e-commerce-report/>

¹⁸⁰ <https://www.statista.com/study/42335/ecommerce-report/>

¹⁸¹ <https://www.statista.com/study/42335/ecommerce-report/>

¹⁸² <https://www.netimperative.com/2018/05/23/european-digital-advertising-market-has-doubled-in-size-in-5-years/>

¹⁸³ <https://www.statista.com/statistics/307005/europe-online-ad-spend/#:~:text=ln%202022%2C%20digital%20advertising%20spending,stood%20at%2092%20billion%20euros.>

¹⁸⁴ <https://www.consilium.europa.eu/en/infographics/platform-economy/>

¹⁸⁶ <https://www.telecoming.com/blog/subsconomics-the-subscription-economy-will-surpass-228-billion-during-2021/>

	<p>Growth was driven by increased consumer take-up of subscription services across sectors including media, software, and consumer goods.</p> <p>A report by ING and Bernstein, the European subscription economy was valued at around €20 billion in 2016.</p> <p>2018 - ING estimated that Europeans spend EUR 80 billion a year on subscriptions for goods, durable goods around € 50 billion a year; and consumable goods €30 billion).¹⁸⁵ However, the total estimated European subscription economy size is c.a. € 350 billion once services are factored in.</p> <p>ING estimated that the average household spends € 130 monthly on all subscriptions and 5% of European household consumption spent on subscriptions.</p>	<p>By 2023, the subscription economy had grown substantially in Europe and globally by more than 300% in the past seven years, reflecting a robust expansion trend. 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.¹⁸⁷</p> <p>In 2023, the subscription economy in Europe had turnover of approximately €199.4 billion (eCommerce Europe). This figure represents the significant and ongoing growth of the subscription-based business models across various sectors, including media, software, and consumer services. The trend continued, with projections indicating a substantial increase to €330.58 billion by the end of 2024, driven by the convenience and personalisation of subscription services, and the increasing shift towards digital and online consumption.¹⁸⁸</p> <p>Services dimension of subscription economy continues to outstrip subscription for goods.</p>
European gaming industry and loot boxes	<p>Turnover estimated in European video games market and loot boxes:</p> <p>2018 - €21 billion for European video games market, of which €7.14 billion resulting from in-app purchases and paid apps, including loot boxes.¹⁸⁹</p>	<p>Turnover estimated in European video games market: 2022 - €24.5 billion.</p> <p>Globally, revenue generated from loot boxes used in video games could exceed \$20 billion (€18.4 billion) by 2025 (Juniper Research). EU-27 to be worth some €3-4 billion per annum based on Europe's market share of global turnover.</p>
Virtual worlds/metaverse	<p>The metaverse was considerably smaller in 2016-17 as most market developments have taken place in the last 3 years only, given its nascent nature.</p>	<p>The Brainsights¹⁹⁰ in 2022, the global metaverse market is expected to grow from €36.3 billion in 2021 to €918.2 billion by 2030.</p>

3.2.2.1 Ecommerce

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 device, varying store concepts and business models, and innovative arrangements and relationships between consumers, traders and intermediaries. According to Christel Delberghe, Director-General of Ecommerce Europe, a forthcoming study expects online sales to make up an average of 30% of retail turnover by 2030.¹⁹¹ Key market highlights:

- In 2023, the global e-Commerce market will cross the two trillion US\$ threshold (€1.84 trillion).¹⁹²

¹⁸⁵ https://think.ing.com/uploads/reports/Subscriptions_from_music_to_tools_and_toiletries_ST_ING_Economics_April_OT.pdf

¹⁸⁷ <https://www.businesswire.com/news/home/20190321005245/en/The-Subscription-Economy-Grows-More-Than-300-In-The-Last-Seven-Years>

¹⁸⁸ <https://ecommerce-europe.eu/wp-content/uploads/2023/11/European-Ecommerce-Report-2023-Light-Version.pdf#:~:text=URL%3A%20https%3A%2F%2Fecommerce>

¹⁸⁹ 2018 trends and data ISFE, European Video Games Industry, Market size data is extracted from Newzoo | 2018 Global Games Market - <https://videogameseurope.eu/wp-content/uploads/2019/08/ISFE-Key-Facts-Brochure-FINAL.pdf>

¹⁹⁰ Brainsights, 2022. Metaverse market size. Available at: <https://www.thebrainsights.com/report/metaverse-market>

¹⁹¹ S. Lone and J.W.J. Weltevreden (2022) *2022 European E-commerce Report*. Amsterdam/Brussels: Amsterdam University of Applied Sciences & Ecommerce Europe. Available at: <https://www.eurocommerce.eu/app/uploads/2022/08/European-E-Commerce-Report-2022-LIGHT-VERSION.pdf>. p.3

¹⁹² eCommerce report 2023, Statista, January 2023. <https://www.statista.com/study/42335/ecommerce-report/>

- Revenue in the European eCommerce Market is projected to reach US\$632.7bn (€582.7 billion) in 2024, and to show an annual growth rate (CAGR 2024-2029) of 9.1%, resulting in a projected market volume of US\$977.4bn (€900.2 billion) by 2029.

193

Table 3-4 – 2023-2027 e-Commerce market value growth projection:

Region	2023 Market value US\$ billion (EUR)	2027 Market value (US\$ billion) (EUR)	CAGR* growth rate
China	1,156.3 (1065.6)	1,649.4 (1520)	7.4%
USA	904.9 (834.1)	1702.9 (1569.7)	13.5%
EU	662.5 (610.7)	1304.13 (1202.1)	14.5%

*CAGR: Compound Annual Growth Rate / average growth rate per year

Source: Statista 'eCommerce report 2023'¹⁹⁴

Within the EU's single market, e-commerce turnover grew at a rate of between 13-16% in 2021 (according to various data by Statista and Ecommerce Europe), 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 smart phones.¹⁹⁵

Regarding the prevalence of participation in e-commerce transactions by European consumers, according to Eurostat, 75% of internet users bought or ordered goods or services online in the EU in 2023. Using as the denominator the total number of individuals who used the internet in the last three months before the survey, the proportion of e-shoppers reached 75 % in 2023, an increase from 57 % (+18 pps) in 2013.¹⁹⁶ Regarding how far consumers are affected by age group, a generational divide has been observed between age groups in the analysis performed by Eurostat. *"The shares of the age groups 16-24 years, 25-34 years and 35-44 years were over the EU average while the age groups 55-64 years and 65-74 years were below the average"*. In 2023, the proportion of the population that used the internet in the 12 months prior to the survey, bought or ordered goods or services on the internet was 87 % for individuals aged 25-34 years, 84 % for those aged 35-44 years, 82 % for those aged 16-24 years and 75% for those aged 45-54 years, 55-64 years was 65 % and 65-74 years 60 %.¹⁹⁷ According to other Eurostat data presented in ecommerce Europe's annual European e-commerce report, the percentage of internet users who bought goods and services online increased from 81% in 2018 to 87% in 2023.¹⁹⁸ According to ecommerce News, ecommerce in Europe (online sales of goods and services) was estimated at €509.9 billion in 2016.

It is important to note from a regulatory, but also from an economic and social perspective, that SMEs are reported as lagging behind large firms in terms of their use of digital tools, something that may gain greater salience as e-Commerce market value continues to grow.

¹⁹³ <https://www.statista.com/outlook/emo/e-commerce/europe>

¹⁹⁴ eCommerce report 2023, Statista, January 2023. <https://www.statista.com/study/42335/e-commerce-report/>

¹⁹⁵ Lone and Weltevreden (2022) *2022 European E-commerce Report*. p.1, 13.

¹⁹⁶ Internet users who bought or ordered goods or services for private use in the previous 12 months by age group, EU, 2010-2023 (% of individuals who used internet in the previous 12 months) Source: Eurostat ([isoc_ec_ibuy](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals&oldid=629584#:~:text=)%20and%20(isoc_ec_ib20)-,75%20%25%20of%20internet%20users%20bought%20or%20ordered%20goods%20or%20services,%2C%20from%2057%20%25%20in%202013)) and ([isoc_ec_ib20](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals&oldid=629584#:~:text=)%20and%20(isoc_ec_ib20)-,75%20%25%20of%20internet%20users%20bought%20or%20ordered%20goods%20or%20services,%2C%20from%2057%20%25%20in%202013)) - [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals&oldid=629584#:~:text=\)%20and%20\(isoc_ec_ib20\)-,75%20%25%20of%20internet%20users%20bought%20or%20ordered%20goods%20or%20services,%2C%20from%2057%20%25%20in%202013](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals&oldid=629584#:~:text=)%20and%20(isoc_ec_ib20)-,75%20%25%20of%20internet%20users%20bought%20or%20ordered%20goods%20or%20services,%2C%20from%2057%20%25%20in%202013).

¹⁹⁷ Idem. Eurostat, 2023 – e-commerce statistics for individuals

¹⁹⁸ <https://ecommerce-europe.eu/wp-content/uploads/2023/11/European-Ecommerce-Report-2023-Light-Version.pdf>

For consumers, the most significant perceived barrier to online shopping across the EU-27, according to the 2022 European E-commerce report, was consumer preference to shop in person, to see products, loyalty to shops or force of habit (54%); with payment security or privacy (18%) featuring as a secondary concern of varying significance across Member States.¹⁹⁹

Increasing access to the internet, particularly through mobile devices, has not only underpinned e-Commerce growth in the EU, but also globally.²⁰⁰ Statista's 2023 report predicts continued digital transformation of eCommerce, driven by cashflow and innovation from fast-developing Asian economies.

3.2.2.2 Digital advertising

The **global digital advertising market** is a significant sector within digital markets and services. Its growth has been accelerated by big data. Data on this sector is relevant as it provides contextual background when considering topics such as personalised advertising and pricing, which are more prevalent in this sector and is also component of the broader platform economy (see separate section below).

Global turnover is above USD 549.5 billion in 2022, with projections for further growth in future (Statista).²⁰¹ The European digital advertising market reached an estimated €86 billion in 2022 (IAB Europe), having grown by 9.8% in 2022, down from 31% growth in 2021, driven by the switch to online advertising and shopping during the pandemic.²⁰² According to Statista, the Digital Advertising market worldwide is projected to grow by 6.87% (2024-2028) resulting in turnover of US\$96.6bn in 2028. The means through which Digital Advertising will be spent will also shift, with an increase to 70% of total ad spending will be generated through mobile in 2028.²⁰³

The digital advertising market within the EU, and was valued at around €41.9 billion in 2016, and was estimated to be worth €86 billion by 2022. The Digital Advertising market in Europe is projected to grow by 6.0% (2024-2028) resulting in a market volume of US\$161.2bn (€148.7 bn) in 2028. It can be noted that in 2023 and 2024, there has been a slowdown in spending on digital advertising as the post-pandemic situation has normalised. Whilst personalised ads account for a significant market share, it is difficult to obtain disaggregated data within total digital advertising spend. However, qualitative feedback was received that most ads are personalised and that consumers appreciate more relevant content, though this raises concerns for consumer protection examined in the case study). There are examples of more specialised markets relevant to the topic of personalised ads. For instance, the global Artificial Intelligence in Personalised Marketing Market size was valued at USD 1.18 billion in 2023. This is expected to increase in size by 27.1% CAGR in the 2023-2030 period.²⁰⁴

3.2.2.3 Platform economy

A definition of the platform economy is "the tendency for commerce to increasingly move towards and favour digital platform business models. Platforms are underlying computer systems that can host services that allow consumers, entrepreneurs, businesses and the general public to connect, share resources or sell products".²⁰⁵ A legal definition has also been

¹⁹⁹ Ibid.

²⁰⁰ eCommerce report 2023, Statista, January 2023

²⁰¹ <https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/>

²⁰² https://iabeurope.eu/wp-content/uploads/2023/07/IAB-Europe_AdEx-Benchmark-2022_REPORT-1.pdf

²⁰³ <https://www.statista.com/outlook/dmo/digital-advertising/worldwide>

²⁰⁴ AI in Personalized Marketing Market - <https://www.futuredatastats.com/artificial-intelligence-in-personalized-marketing-market>

²⁰⁵ Laura Fitzsimmons - <https://www.techtarget.com/searchcio/definition/platform-economy>

provided in the DSA regarding different types of platforms, through the adoption of a designation of very large online platform (VLOP)²⁰⁶, with more than 45 million users/month. There are many different types of online platforms, ranging from those that provide intermediary services used by consumers daily, such as Uber and Airbnb and digital food delivery services, to platforms that are also used to provide digital labour services. Regarding the different types of platform-focused business models, there are three major types of platform within the platform economy:²⁰⁷

- **Transaction platforms** - virtual marketplaces and meeting places such as Amazon, Etsy and Facebook.
- **Innovation platforms** - provide technology frameworks to customers adapted to individual use. Examples of innovation platform companies include Microsoft.
- **Integration platforms** - a combination of transaction and innovation platforms, similar to online application marketplaces such as the Apple App Store or Google Play.

The platform economy includes both Business to Consumer (B2C) and Business to Business (B2B). Given the study focus on EU consumer law, the focus is only on B2C in this study, although it can be noted that there are new rules for platform-to-business trading practices²⁰⁸, affecting B2B. Whilst C2C is a growing trend in digital markets, due to the rapid increase in size of platforms that allow C2C, such as eBay and Vinted, consumer sellers are not subject to EU consumer law, Provided they are individual sellers and not professional sole traders.

The EU Observatory on the Online Platform Economy²⁰⁹ monitors and analyses the latest trends and data of the online platform economy. The platform economy was defined broadly in a scoping study as including (1) e-commerce marketplaces, (2) online application stores, (3) online search engines, (4) social media platforms, and (5) online media platforms.²¹⁰ The observatory was only recently set up, and there presently appears to be a lack of reliable and comprehensive official EU statistics on the platform economy, hence one of the new observatory's functions is to strengthen measurement of the platform economy. The absence of statistics is because the concept of the platform economy covers many different areas of digital markets and services. Moreover, it can be noted that e-commerce also lacks official statistics, hence why Digital Europe and EuroCommerce produce annual statistics of their own (see earlier Section 3.2.1).

Size of the EU's platform economy

According to Eurostat data, the EU's platform economy has grown exponentially from an estimated €3 billion in 2016 to €14 billion in **annual revenues** by 2020.²¹¹ On the assumption that growth has continued during the 2021-24 period, it can be estimated that with a growth rate of approximately 8-10% per annum, this estimate had increased to €19 billion by 2024.

Data estimates of the size of the platform economy were also obtained for the value by **market capitalisation**. 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 \$314.60 billion (USD) 290.2 billion (Platform

²⁰⁶ The DSA classifies platforms or search engines that have more than 45 million users per month in the EU as very large online platforms (VLOPs) or very large online search engines (VLOSEs). The Commission has begun to designate VLOPs or VLOSEs based on user numbers provided by platforms and search engines. However, market research reports define the platform economy as including small platforms

²⁰⁷ Adapted from <https://www.techtarget.com/searchcio/definition/platform-economy>

²⁰⁸ The EU Regulation on platform-to-business relations (P2B Regulation) is the first set of rules for creating a fair, transparent and predictable business environment for smaller businesses and traders on online platforms. <https://digital-strategy.ec.europa.eu/en/policies/platform-business-trading-practices>

²⁰⁹ [Observatory on the Online Platform Economy \(platformobservatory.eu\)](https://platformobservatory.eu)

²¹⁰ European Commission, (2018) Study on "Support to the Observatory for the Online Platform Economy", DG CNECT and DG GROW, by PPMI, Open Evidence, Rand Europe.

²¹¹ <https://www.consilium.europa.eu/en/infographics/platform-economy/>

Economy.io).²¹² A Report in the US identified 370 top 'digital platforms' globally representing an estimated annual revenue of \$1.87 trillion and 371 billion average monthly users in 2022.²¹³ Whilst Europe has a strong platform economy, the important role of big tech and global firms in the platform economy should be highlighted as Europe only has nine major platforms. Europe's market share in annual turnover is only approximately 0.1% (€19 billion compared with the above estimate of \$1.87 trillion).

Some research suggests that Europe needs to do more to strengthen its market share in the platform economy.²¹⁴ BearingPoint consultancy notes that *"out of a total of USD 4.3 trillion globally, Europe can currently claim only 200 billion of market capitalisation — that is, less than 5%"*. This is reflected in the number of listed platforms. According to the same research, the UK has only 8 and Germany 4 compared with 82 in China. The U.S. also clearly dominates the market in terms of global platform providers such as Facebook and Google (owner of YouTube).

Especially with respect to large platforms (those with over 100,000 EUR in revenue and over 1,000,000 customers and service providers per platform), nearly half of the global industry's annual turnover is located in the U.S., given platforms are dominated by a number of global leaders. According to research by the JRC, while examining the proportion of platforms with a local origin for each MS, except Bulgaria and Slovakia, fewer than 50% of all platforms operating in a given European country had a domestic origin. All recognised platforms are of foreign origin in smaller national economies of Member States such as Cyprus, Latvia, Luxembourg, and Slovenia. The fact that over 40% of the identified platforms are available in two or more languages, often the local language and English, further supports the concept that the platform economy is largely transnational. However, platform workers make up a sizable portion of the labour force in the EU (28.3 million in 2022), considering the 29 million workers in manufacturing. This number is anticipated to expand quickly and reach 43 million in 2025, representing a 52% increase in only three years.

3.2.2.4 Subscription economy

Key highlights are:

- The exponential growth in the past five years of the global digital subscription economy, powered by digital product and service subscriptions. The market is dominated by the US, but the EU also has a rapidly-growing subscriptions market.
- Online subscriptions – including their automatic renewal – has become an increasingly prevalent business model. Free trials that convert to a paid subscription at the end of the trial to an automatic renewal are also a growing market. There is some crossover between other areas of digital markets and services, such as digital platforms, which have been experimenting with subscription models (e.g. in 2023, Facebook and X introduced subscriptions – see subscriptions case study).
- New types of subscriptions are emerging due to the maturation of social media platforms and the evolution in business models of content creators (e.g. freemiums, micro contracts signing up for additional paid-for / members only content).

Market size of the European subscription economy

Market estimates in 2020 valued the global digital subscription economy at 650 billion USD (€598.2 billion), with an expectation that the market's rapid growth will continue, exceeding

²¹² <https://www.platformeconomy.io/blog/platform-economy-2023-u-s-leads-europe-lags>

²¹³ <https://www.dinarstandard.com/post/global-digital-platform-powerindex-2023>

²¹⁴ <https://www.bearingpoint.com/en/insights-events/insights/can-europe-be-a-player-in-the-platform-economy/>

twice this value by 2025, which is projected to be \$1.5 trillion.²¹⁵ Market sub-segments include durable goods and consumer goods through e-commerce and subscription services, including cloud-based subscriptions.

According to a Deloitte study in 2018, the global digital subscription market is dominated by the US,²¹⁶ accounting for over half of the global market, followed by Europe (21% or €78.6 billion) and China (14%), respectively.²¹⁷

In 2018, ING estimated that Europeans spend EUR 80 billion a year on subscriptions for goods, durable goods around € 50 billion a year; and consumable goods €30 billion). However, the total estimated European subscription economy size is c.a. € 350 billion once services are factored in.²¹⁸

Regarding the evolution in the current baseline situation, by 2023, the subscription economy in Europe had turnover of approximately €199.4 billion (eCommerce Europe). This figure represents the significant and ongoing growth of the subscription-based business models across various sectors, including media, software, and consumer services. The trend continued, with projections indicating a substantial increase to €330.58 billion by the end of 2024.

According to *Transparency Market Research*, “the major vendors that offer digital subscription are Salesforce, Amazon, Flipkart, TechCrunch, Netflix, Microsoft Corporation, Algolia, Oracle Corporation, SAP SE, and Vigorate Digital Solutions. These leading companies are focusing on inventing new technologies and expansion for growth in digital subscription markets.”²¹⁹

Research by ING suggests that the average European household spends 130 EUR per month on all subscriptions, for an estimated market value of €350 billion, 5% of total European household consumption. Regarding the combined market value of service subscriptions (such as internet, mobile phone services or cable TV), this accounts for 240 billion EUR in value. Meanwhile, purely digital product and service subscriptions (such as software, music, video-on-demand and games) are valued collectively at €30 billion. Importantly, the latter category is outstripping tangible goods subscriptions and expected to grow further, with young Europeans continuing to subscribe at a higher rate.²²⁰

According to a research paper by industry representatives in Scandinavia, the subscription business model has grown exponentially in recent years. “Globally, the total number of companies offering a service based on subscription is estimated to be around 28,000”.²²¹

In recent years, the online subscription economy has also seen new developments to their business models, which include:

- **The changing nature of monetisation business models used by content creators on online platforms.** Consumers may choose to support their favourite content creator by signing up for additional paid-for services / members-only content by making a one-off or regular monthly micro payment contribution through membership sites

²¹⁵ [Subscription economy: global market size 2025 | Statista](#) ; [The subscription prescription \(deloitte.co.uk\)](#)

²¹⁶ [The subscription prescription \(deloitte.co.uk\), 2018](#)

²¹⁷ [Subscription economy: global market share 2020 | Statista](#)

²¹⁸ https://think.ing.com/uploads/reports/Subscriptions_from_music_to_tools_and_toiletries_ST_ING_Economics_April_OT.pdf

²¹⁹ [Subscription \(Digital\) Services Market Scope, Size, Share, Trends, Forecast, Analysis by 2026 \(transparencymarketresearch.com\)](#)

²²⁰ 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. <https://www.ing.nl/media/ING_EBZ_opportunities-and-challenges-for-tangible-goods-subscriptions_tcm162-143372.pdf>

²²¹ SUBSCRIPTION ECONOMY: BUSINESS PERSPECTIVE - https://www.nets.eu/SiteCollectionDocuments/white-paper/whitepaper_subscription_economy_business_perspective.pdf

such as Patreon²²² and Buy Me a Coffee²²³ promoted through online platform content.

- **The trend towards freemium business models for online services. Basic services are provided free of charge, whilst consumers pay for advanced features and services.** Whereas many platforms have previously relied solely on advertising-based business models, with consumers benefiting from personal data paid 'free' services, there is a trend towards subscription services for a certain percentage of customers willing to pay for premium services. In 2022-23, for instance, both X (Twitter Blue) and Meta (META Verified) have launched or are testing subscription services²²⁴.

These examples highlight how increasingly-complex relationships and modes of business may require further consideration by regulators in open discussion with all stakeholders. However, this does not preclude that other developments may also occur more rapidly and sporadically with potential implications relating to consumer safety. As an example, X (formerly Twitter) is considering disabling two-step authentication for non-subscription, verified users which could undermine cybersecurity and expose consumers to online harms.

3.2.2.5 Virtual worlds

Metaverses or virtual worlds are becoming more and more popular and influential in Europe as well as globally. Metaverses/virtual worlds can also be broken down into two categories: a virtual metaverse (a fully simulated world) and an augmented metaverse (layers of virtual content that are overlaid upon the real world with precise spatial registration). Metaverses can often involve the use of virtual reality, augmented reality, and other advanced technologies.²²⁵

According to a market research report by the Brainy Insights²²⁶ in 2022, the global metaverse market is expected to grow from €36.3 billion in 2021 to €918.2 billion by 2030. In the same vein, according to Gartner²²⁷, a technological research and consulting firm, by 2026, 25% of people will spend at least an hour daily in the metaverse for work, shopping, education, social activities and/or entertainment.

Metaverses/virtual worlds are sometimes seen as a possible next-generation of the internet; a new way in which individuals will engage with the internet. It could mean activities occurring currently on the internet, occurring instead in a shared 3D immersive space. In this 3D space, people can interact, transact, and participate in virtual activities.²²⁸ The European Commission²²⁹ is aware of the opportunities and challenges that metaverses present and issued a Communication on virtual worlds in July 2023²³⁰. The initiative aims to ensure that metaverses reflect EU values and fundamental rights, foster innovation for businesses and create interoperable standards among different platforms. Metaverses/virtual worlds infrastructure includes network connectivity like Wi-Fi, 5G, cloud systems, and even Microelectromechanical Systems (MEMS), but is also dependent on physical infrastructure

²²² <https://www.patreon.com/> - a website site that enables creators to build memberships by providing exclusive access to their work.

²²³ <https://www.buymeacoffee.com/>

²²⁴ See *inter alia*: <https://www.euronews.com/next/2023/02/20/meta-verified-meta-emulates-twitter-with-paid-subscription-service-for-facebook-and-instagram> and <https://techwireasia.com/2023/02/meta-unveils-twitter-blue-like-subscription-are-paid-subscriptions-the-next-step-for-social-media/>

²²⁵ World Economic Forum, 2022. 3 technologies that will shape the future of the metaverse – and the human experience. Available at : <https://www.weforum.org/agenda/2022/02/future-of-the-metaverse-vr-ar-and-brain-computer/>

²²⁶ Brainy insights, 2022. Metaverse market size. Available at: <https://www.thebrainyinsights.com/report/metaverse-market>

²²⁷ Gartner, 2022. Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026. Available at: <https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026>

²²⁸ TechTarget, 2022. What is the metaverse. An explanation and in-depth guide. Available at: <https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know#>

²²⁹ European Commission, 2023. Virtual Worlds fit for people. Available at: <https://digital-strategy.ec.europa.eu/en/policies/virtual-worlds>

²³⁰ <https://digital-strategy.ec.europa.eu/en/policies/virtual-worlds>

like Graphics Processing Unit (GPU) cores which process metaverse data.²³¹ Market highlights are that:

- The metaverse market is expected to grow rapidly in the coming years, as more people and businesses seek immersive and interactive experiences in the virtual world.
- Factors driving market growth are the increasing adoption of online gaming and e-sports, rising demand for social media and entertainment platforms, growing investments in blockchain and NFTs, and the emergence of new players and partnerships in the metaverse space.
- For instance, in December 2021, Facebook rebranded itself as Meta and announced its vision to help bring the metaverse to life.²³²
- In January 2022, Microsoft proposed to acquire Activision Blizzard, one of the largest gaming companies in the world, to expand its building blocks for the metaverse.²³³
- In November 2021, Nike partnered with Roblox to create a virtual world called Nikeland, where users can dress up their avatars with Nike's branded sneakers and apparel.²³⁴
- Qualcomm has established a €88 million metaverse fund to further develop VR and AR technologies.²³⁵
- Users are also starting to invest in the metaverse. Recently, one user bought a piece of land²³⁶ in the virtual world Sandbox for €3.7 million (i.e. the biggest purchase in the Metaverse so far).

3.2.2.6 European video games industry and loot boxes

In 2018, the European video game market was worth EUR 21 billion, with a 15% year-on-year growth rate. The Interactive Software Federation of Europe (ISFE) estimates 34% of turnover (i.e. €7.14 billion) resulting from in-app purchases and paid apps, including loot boxes.²³⁷ Fully disaggregated data on loot boxes alone was not available.

Revenue generated by the video games industry in 2022 across five key markets was €24.5 billion. The video games industry employed 110,000 people in Europe in 2022. Regarding revenue split by source: 17% physical revenue (physical copies of games) 41% online revenue (game downloads etc), and 41% app revenue. Juniper Research has found that revenue generated from loot boxes used in video games will exceed \$20 billion by 2025.²³⁸ This suggests that the value of loot boxes has increased exponentially globally. In Europe, data was lacking on estimates of loot boxes value. However, a call for evidence found that the loot box market was estimated to be worth £700mn (€812 million) in the UK in 2019. On the basis

²³¹ Ericsson, 2022. What is the metaverse and why does it need 5G to succeed? The metaverse 5G relationship explained. <https://www.ericsson.com/en/blog/2022/4/why-metaverse-needs-5g>

²³² Meta, 2021. Introducing Meta: A Social Technology Company. Available at: <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/>

²³³ Microsoft, 2022. Microsoft to acquire Activision Blizzard to bring the joy and community of gaming to everyone, across every device. Available at: <https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/>

²³⁴ Reuters, 2021. Into the metaverse: Nike creates 'NIKELAND' on Roblox. Available at: <https://www.reuters.com/technology/into-metaverse-nike-creates-nikeland-roblox-2021-11-18/>

²³⁵ Qualcomm, 2022. Qualcomm Launches \$100M Snapdragon Metaverse Fund. Available at: <https://www.qualcomm.com/news/releases/2022/03/qualcomm-launches-100m-snapdragon-metaverse-fund>

²³⁶ The Guardian, 2022. Digital land grab: financial speculation in the metaverse. Available at: <https://guardian.ng/news/digital-land-grab-financial-speculation-in-the-metaverse/>

²³⁷ [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU\(2020\)652727_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU(2020)652727_EN.pdf)

²³⁸ <https://www.juniperresearch.com/press/video-game-loot-boxes-to-generate-over-20-billion/>

of these two estimates, the study team has estimated loot boxes in the EU-27 to be worth some €3-4 billion per annum.

3.2.3 Costs and benefits for traders

3.2.3.1 Costs for traders

EQ6 – What are the regulatory compliance costs (administrative, adjustment costs) of the Directives for the traders?

The costs supported by traders include both adjustment and administrative costs. There will be some adjustment costs from having to redesign processes or websites to ensure compliance but the consultations (e.g. enterprise survey, interviews) suggested that these costs are not significant if the changes are designed-in from the outset. If conversely, design changes need to be made retrospectively to websites, apps or platforms, these are more costly, but would primarily stem from non-compliance with existing obligations.

The estimated costs mainly focused on the **general adjustment and administrative costs for traders in the digital environment of complying with EU consumer laws**. The estimates include digital-specific provisions of which there are presently very few, mainly those applicable to e-commerce traders under the CRD and the recent changes introduced through the MD, such as information disclosures applicable to marketplaces and the prohibition of some digital practices such as the use of scalping bots for event tickets. Whereas in future, if more specific digital rules were introduced, there would be digital-specific compliance costs, most costs of complying with EU consumer law relate to traders applying long-existing rules in the digital environment.

The enterprise survey revealed that only a small percentage of companies incurred compliance costs; with only **10% of traders reporting additional (or higher) costs** from adjusting practices and **15% for checking compliance**/administrative costs. This is reasonable, considering the perception that the regulatory framework has been in place for a long time and therefore, many compliance costs were one-off and experienced a long time ago, as there are high levels of familiarity with the core set of consumer law rules among many traders. The answers are likely to reflect the view of those new traders entering the market and/or changing to online trading practices which are fewer in number than those already operating digitally.

A higher percentage of traders thus highlighted low costs or no costs at all. Low costs have not been included in the overall calculations. This is because traders only focus on the most significant costs when making business decisions and entering the market. There is thus an implicit assumption that, for these last group of traders, the benefits will outweigh the cost and that they have been able to absorb the costs with low impact to their activities under a business-as-usual scenario. There is of course a risk that the total costs may be an underestimate but this is expected to be low. Moreover, this approach is more in line with the **proportionality** principle²³⁹, where cost estimates are prioritised for initiatives that entail significant costs. Costs data triangulation has also been included in the approach to validate the estimates and add more rigour (see section **Error! Reference source not found.**).

The adjustment costs have been estimated at a range of between **EUR 208m and EUR303m across the EU. The total administrative costs of checking compliance have been estimated at EUR 249.8m to EUR487.5m.**

There were found to be **limited digital-specific regulatory requirements in EU consumer law**. As these were very recent, they were difficult to quantify, as many changes stemmed through the MD or even more recently, the introduction of the right of withdrawal button in the CRD through the Distance Marketing of Financial Services Directive.

New digital-specific information obligations for marketplaces introduced in 2022 through the MD only resulted in modest one-off compliance costs. These mainly require useful information (but limited in

²³⁹ This refers to the proportionality of the analysis, according to Better Regulation Guidelines (Toolbox 12) and not to the proportionality principle regarding whether the initiative has achieved its objectives at the lowest possible costs and with the lowest possible resources.

volume) to be provided to consumers, such as regarding general criteria used in search engine rankings and information as to whether a price has been personalised. This requires some adjustment costs to design-in pop-up boxes providing information disclosures but these are increasingly required across a range of different pieces of EU (and sometimes also national) legislation. The costs were seen as proportionate.

There are also longstanding pre-contractual information requirements in the CRD, which apply to e-commerce traders (as well as to offline distance contracts such as doorstep selling).

The consultation feedback from this fitness check revealed differences in the perceptions of costs by traders between different survey tools; with the targeted consultation showing larger costs. The sample size is however considerably smaller than the enterprise survey. Because of this, the enterprise survey has been used as the main source for the assumptions.

EQ6(1) – What is the cost for businesses to comply with the Directives, including specifically for SMEs considering different kinds of SMEs operating in the digital sector(s) by size threshold (micro, small and medium firms)?

Traders must comply with EU consumer law whether in the digital environment or offline. In this section, given that there are very few digital-specific requirements in EU consumer law due to its technology-neutral nature, the general costs of applying EU consumer law by traders operating digitally and/ or multi-channel are considered. However, there are a few digital-specific requirements that have been recently introduced, such as several changes made through the MD. For instance, under the MD, information obligations for platforms and marketplace carry both administrative costs and adjustment costs. The Directive requires online traders to provide consumers with details of the criteria to rank search results and, if and, how reviews are verified. This will have different costs implications, and whereas smaller companies may be able to outsource some of these services, larger companies may be able to absorb these within the existing departments.

An overview of the main types of costs of compliance with EU consumer law by traders is provided below. This is based on a combination of desk research to review previous evaluations, the 2017 fitness check and IA studies and interview feedback.

Table 3-5 – Overview of main costs of compliance with EU consumer law by traders

Stakeholders incurring costs (EU consumer law)	Types of adjustment costs	Types of administrative costs
Traders	Familiarisation with rules and obligations and initial compliance planning (e.g., developing compliance strategies) Adjusting business practices e.g. <ul style="list-style-type: none"> • Redesigning an online interface if a trader or CPA identifies dark patterns or other breaches of EU consumer law in the website/app design. • Redesigning business processes for cancellation of contracts/exercising of right of withdrawal. • Change to website/application and other types of interfaces to provide new information required under disclosure rules. 	Checking business’s compliance with legal requirements to ensure that digital commercial practices Information obligations (e.g., pre-contractual and contractual information requirements, disclosure rules under the MD related to information obligations for platforms and marketplaces).

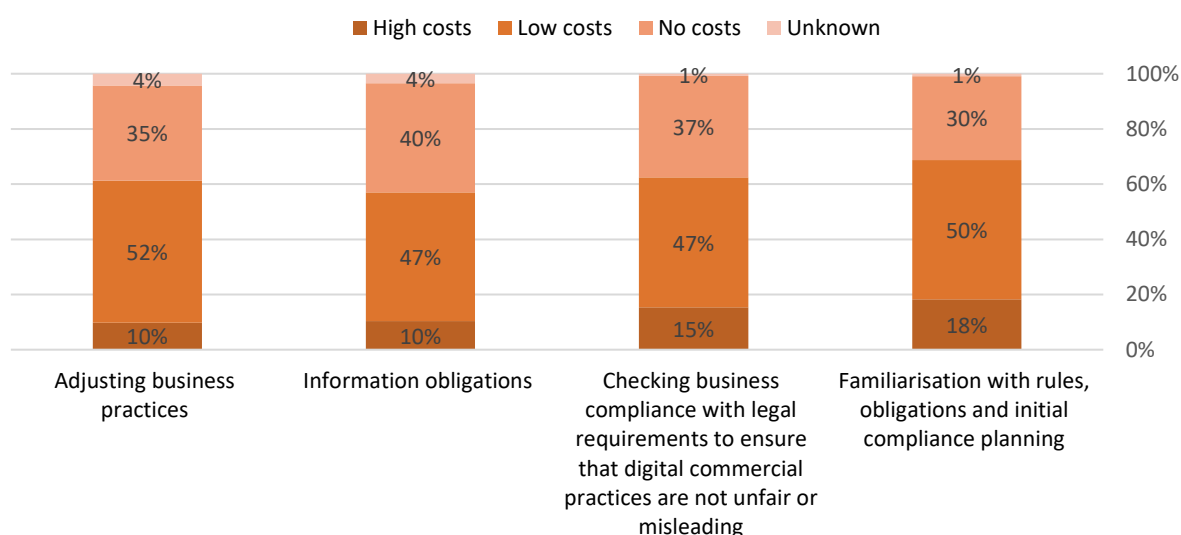
Stakeholders incurring costs (EU consumer law)	Types of adjustment costs	Types of administrative costs
	<ul style="list-style-type: none"> Reengineering business processes. 	

Below we present the findings on costs from the enterprise survey and targeted survey. Some qualitative information from the public consultation is also presented.

Enterprise survey

The enterprise survey of 1000 enterprises in 10 MS asked about the extent of the different costs associated with compliance with EU consumer law in the digital environment. The following figure shows the results.

Figure 3.4 – Costs associated with compliance with consumer law in the digital area (N=1000)



Source: Enterprise survey, Digital Fairness fitness check study

As shown, generally most traders responded that there were low costs or no costs from the current legislative framework across the different types of compliance areas. The findings show that:

Whilst a higher percentage of respondents (18%) indicated high costs for familiarisation with rules, obligations and initial compliance planning compared with the other areas, 30% indicated 'no costs' and 50% stated 'low costs'. There were variations among the sampled Member States, with 29% of companies in Portugal and 26% in Germany and Sweden having experienced high costs and only 5% in Spain and 11% in Romania²⁴⁰.

Regarding checking compliance to ensure that digital practices are not fair or misleading, 37% experienced no costs, 47% some costs and 15% high costs. Again, a higher % of companies experiencing high costs were found in Portugal (25%), this time followed by Poland (23%). Only 7% of companies in Spain and 6% in Romania reported high costs.

Regarding information obligations, 40% experienced no costs, 47% low costs and only 10% high costs. Some of these already existed prior to the MD, such as pre-contractual information obligations under the CRD whereas others were introduced more recently through the MD. It

²⁴⁰ N=100 for each country.

is interesting that the MD amendments to strengthen information disclosure requirements do not appear to have resulted in an in a significant increase in costs. Differences among the companies in MS were smaller than for other requirements.

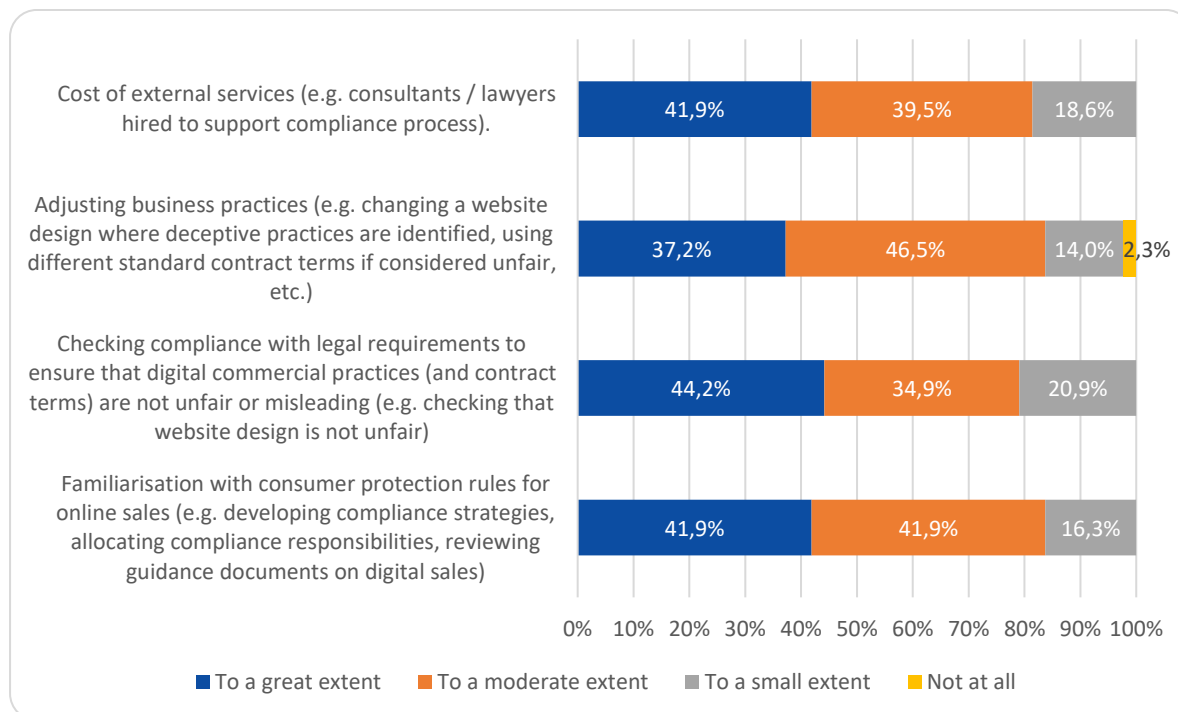
Lastly, turning to adjustments to business practices, 35% experienced no costs, 52% some costs and 10% high costs. Sweden and Poland reported a slightly higher number of companies experiencing high costs than other Member States (16% and 17% respectively).

Targeted survey

Through the targeted survey, an effort was made to gather compliance costs data especially from traders and their representative associations. A total of 83 businesses and trade associations responded to the survey, so the response rate is lower than that of the enterprise survey. However, the data is useful for validation purposes. Among the latter group, c. 24% were operating both offline and online and nearly 18% were e-commerce only. According to the responses, 70% of companies in the sample (N=17) trade across the EU and internationally, which was a significant larger percentage than in the earlier Fitness check²⁴¹ and significantly higher than in the enterprise survey (12%).

The **targeted survey showed different results on compliance costs however**. Over 80% of respondents stated additional compliance costs from the legislation, mostly to do with familiarisation and adjusting business practices, followed by the costs of external services. These results conflict with those of the enterprise survey, but the sample of respondents was considerably smaller, with only 43 responding to this question.

Figure 3.5 – To what extent has compliance with EU consumer law requirements in the digital environment resulted in any additional types of general compliance costs for your business? (n=43)



The survey also asked about the % increase in the additional costs. The largest costs were identified from the familiarisation with consumer protection rules and costs of external

²⁴¹ In the fitness check, only a minority (28 %) of the interviewees sold their products and/or services in other EU Member States and about three quarters (72 %) only operated domestically (see page 43 of SWD).

services. The results are shown in the next Table; but the number of responses (N=16) are rather low to extract conclusive results. Moreover, most of the traders (70%) operated cross-border; so, **differences in MS implementation could explain traders perceptions of a higher level of compliance costs.**

Table 3-6 – Overview of significance of compliance costs according to targeted consultation (N = 16)²⁴²

Stakeholders incurring costs (EU consumer law)	Significant costs (>20%)	Moderate costs (10-20%)	Low costs (5-9.9%)	Very low costs (<5%)
Familiarisation with consumer protection rules for online sales (e.g. developing compliance strategies, allocating compliance responsibilities, reviewing guidance documents on digital sales)	46.7%	53.3%	-	-
Checking compliance with legal requirements to ensure that digital commercial practices (and contract terms) are not unfair or misleading (e.g. checking that website design is not unfair)	37.5%	31.3%	31.3%	-
Adjusting business practices (e.g. changing a website design where deceptive practices are identified, using different standard contract terms if considered unfair, etc.)	31.3%	37.5%	18.8%	12.5%
Cost of external services (e.g. consultants / lawyers hired to support compliance process).	46.7%	33.3%	20.0%	-

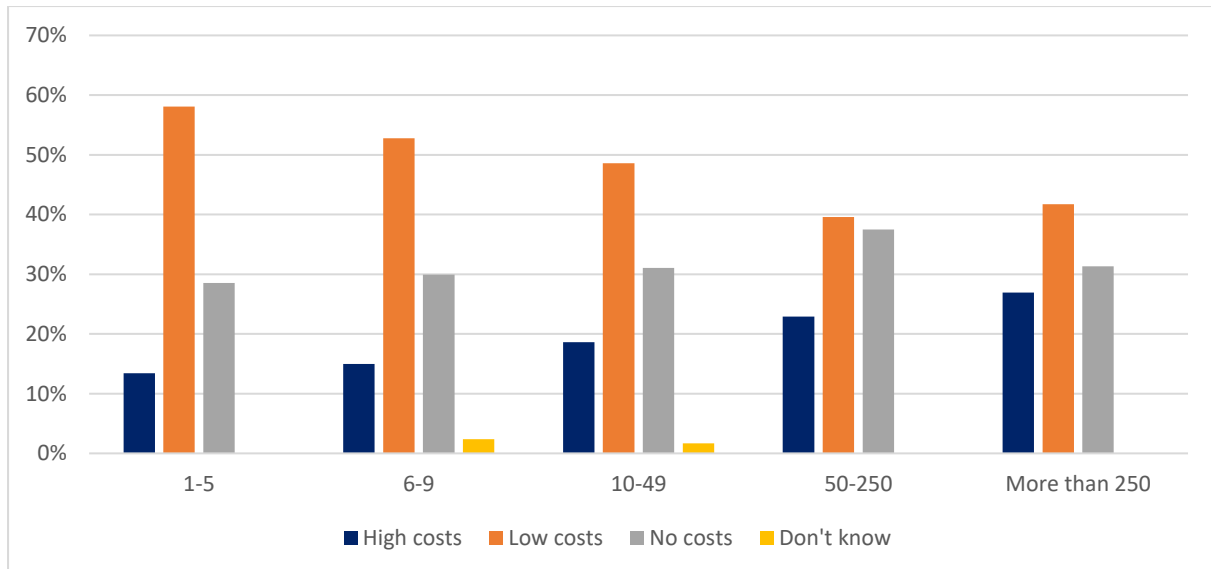
The different types of costs are further described below by company size and sector. Due to the size of the sample, the main source of data is the enterprise survey but validation across the other sources is also provided.

3.2.3.1.1 Adjustment costs

Costs relating to **familiarisation and compliance planning** appear to be low across all company sizes, and particularly among micro-enterprises. 23% of companies with 50-250 employees recorded high familiarisation costs.

²⁴² Q37: If costs have increased to a great or moderate extent, please comment on how significant these additional costs were?

Figure 3.6 – To what extent has compliance with consumer law requirements resulted in familiarisation with rules and obligations and initial compliance planning (e.g., developing compliance strategies) (N = 1000).



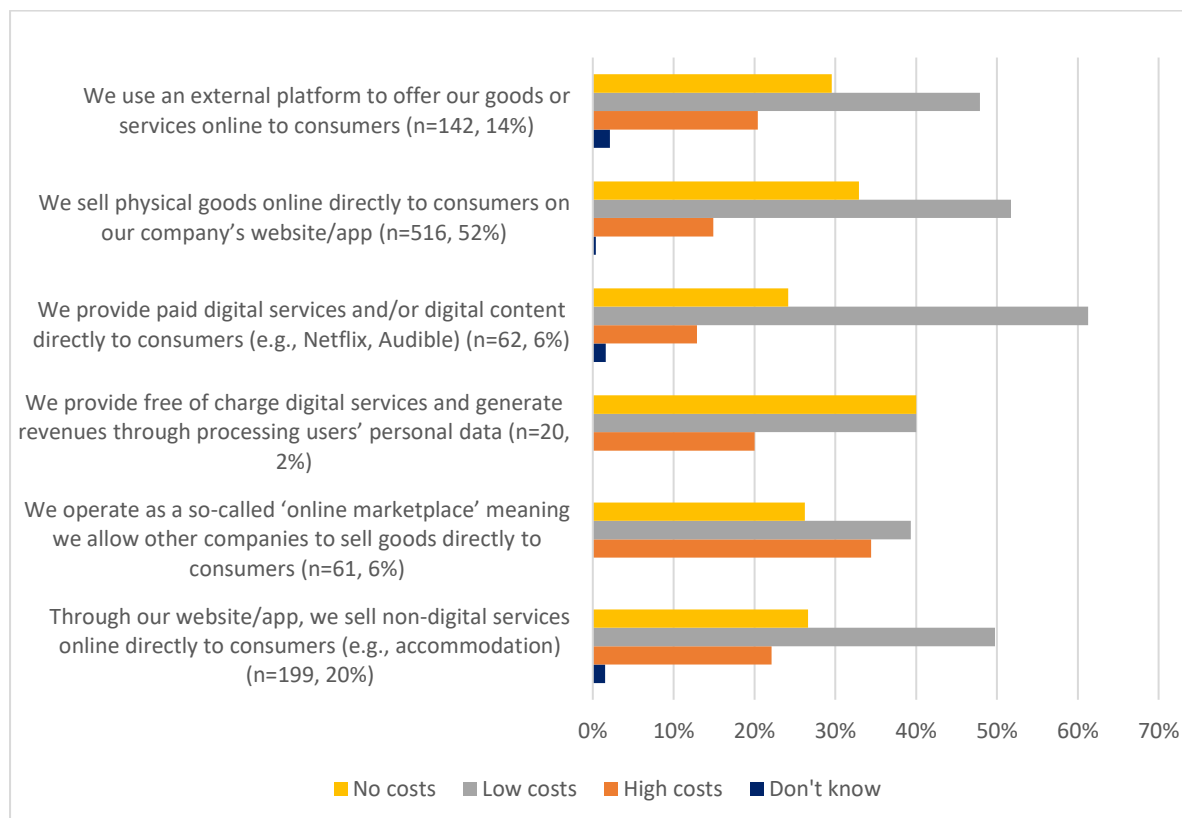
Source: Enterprise survey, Digital Fairness fitness check study

By sector, the largest share of respondents that reported higher costs are within *Retail sale of information and communication equipment in specialised stores* (24%) but 48% of traders within the same sector reported low costs and a further 29% reported no costs. This was followed by the *manufacture of computer, electronic and optical products* (23%). A smaller number of traders in the gas and electricity services sector reported high costs to do with familiarisation (14%).

A more granular assessment of familiarisation costs by type of service is depicted in the next figure. This provides interesting feedback as the responses vary depending on the type of stakeholder. There are interesting differences between different types of traders in their perceptions of familiarisation costs. For instance, online marketplaces viewed familiarisation costs as being high the most frequently (34%). This may reflect the fact that changes were made more recently through the MD that were only applicable to marketplaces and therefore, they perceived there to be higher costs as the regulatory changes led to recent one-off familiarisation costs.

In contrast, among traders selling goods online through a website or app in the e-commerce area, only 15% perceived there to be high costs. However, the recentness of regulatory changes does not always lead to perceptions of high familiarisation costs, for instance, among providers of free digital services, 40% stated there were no costs and a further 40% low costs, whereas 20% reported high costs.

Figure 3.7 – Familiarisation costs with rules and obligations (N = 1000)



Source: Enterprise survey, Digital Fairness fitness check study

For the issue of costs arising from **adjusting business practices**, the majority of respondents indicated low costs (52% of total respondents) or no costs (35%). Companies in Spain (72%) were among the most likely to indicate low costs and at the sectoral level, *Retail sales of telecommunications equipment in specialised stores* (61%) were the sector that indicated low costs most frequently. 45% of companies in France also saw no costs arising from this issue.

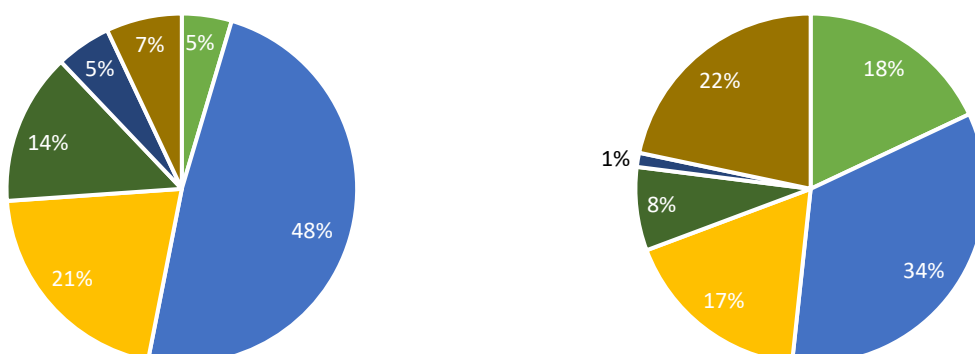
Respondents were questioned about how many employees were dedicated to the initial adjustment of business practices to ensure compliance. They were also questioned on how many days were dedicated to this process and the costs they incurred (if any) to get external advice, mainly legal services. A large percentage of respondents (48%) noted that between 1 and 2 employees were responsible for the adjustment of business practices, with the majority dedicating between **11 and 20 days** as per the following Figure. The most frequent value however was 1 employee (the mode)²⁴³ and the median is 2 employees. The average costs for companies to acquire external services was **EUR 2331 and the median EUR 1600**. The average was greater for Italy however (EUR 2910), within the sector, *Retail sale of telecommunications equipment in specialised stores* (EUR 3055) and companies with 1-5 employees (EUR 2698). It is worth noting that 35% of respondents could not provide a cost estimate and 49% provided a cost of EUR 2,000 or lower, of which 10% reported EUR 2,000 in costs. The rest of the companies (16%) reported greater than EUR 2,000 in costs but they were fewer in number (158 companies).

Figure 3.8 – Initial resources dedicated

Employees working on initial adjustment	Dedicated days to working on business procedures to ensure compliance
---	---

²⁴³ 253 respondents out of 1,000 followed by 232 respondents noting 2 employees.

■ 0 ■ 1-2 ■ 3-4 ■ 5-7 ■ 8-10 ■ Unknown ■ 10 or less ■ 11-20 ■ 21-30 ■ 31-40 ■ 41+ ■ Unknow



Source: Enterprise survey

Due to high BaU costs, companies that operate multi-channel will experience low adjustment costs as they are already familiar with most legal requirements in EU consumer law. However, there were also identified as being some adjustment costs for some types of traders due to having to apply the MD. Examples include changes needed to design the interfaces of marketplaces to comply with new information disclosures, to inform consumers whether a price has been personalised, to inform them whether a trader is an individual or a professional etc. These were considered modest changes (e.g. introducing a hyperlink with a pop-up box on an online interface and providing some basic information). Consequently, **these costs are considered to have been minimal and have not been quantified**. Supporting this, the enterprise survey revealed that 87% of companies reported no or low costs to do with adjusting these practices.

There may be some costs for those companies entering the market that operate online only; as they will have to become familiar with all applicable legislation. In 2021, the EU had 30.1 million enterprises.²⁴⁴ In 2021, **22.8% of traders operated online only**. There are 30.1 million enterprises in the EU and around 5.5m companies in the retail sector.²⁴⁵ The number of companies that could potentially incur some costs to do with adjustment and familiarisation within the retail sector is estimated at 1.25 million (these are enterprises in the B2C domain that operate digitally). Adding the online marketplaces and those in the subscription economy could boost the numbers up to 1.3m. Not all companies will experience costs. The enterprise survey revealed a small percentage of companies incurring compliance costs due to adjustment; with only **10% of traders reported some additional (or higher) costs** from adjusting practices (although with some variations across selling channels and sectors).

Data estimates – adjustment costs for traders

²⁴⁴ [Early 2021 data on businesses more detailed & complete - Products Eurostat News - Eurostat \(europa.eu\)](#)

²⁴⁵ Retail statistics, Eurostat - https://single-market-economy.ec.europa.eu/single-market/services/retail_en. These are expected to reflect B2C businesses. For comparison, in 2017 it was estimated that there were 930,000 business were selling online domestically and 400,000 businesses were selling on-line cross-border (source: CEC (2017): Commission Staff Working Document on the Impacts of fully harmonised rules on contracts for the sales of goods supplementing the impact assessment accompanying the proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods).

There are two different estimates of adjustment costs for traders. The first relates to traders that have dealt with managing compliance in-house. 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).

Applying the same 10% and a value of **EUR 1,600 in adjustment costs**²⁴⁶ for these companies (based on the median)²⁴⁷, the adjustment costs can be estimated at **EUR 208m across the EU**; and

If a higher **average value** were to be assumed of the adjustment costs (which also includes the costs of hiring external services is EUR 2,331), **then total costs would increase to EUR 303m.**

Adjustment costs would mainly be one-off costs, though not exclusively, as there may be some recurrent costs. An example is that prior to new T&Cs being published, even if a trader has already complied with the UCTD previously, the new T&Cs will need to be carefully checked for any potential standard unfair contract terms.

There can also be more costly types of adjustment costs, such as having to make major changes to a design interface upon complaint from consumers and/ or from enforcement authorities due to failing to comply with the UCPD's requirements on dark patterns. Such costs could be significant, with a significant range of costs. The costs incurred will depend on the size of the business concerned. It could vary from a days' reprogramming work and consultations between web design teams and compliance managers through to major design interface overhauls for major traders. It is therefore difficult to generalise about costs, but a range of EUR 10,000 – 20,000, which is the ranges of the highest values given in the enterprise survey. However, where incurred, such costs would be due to non-compliance with EU consumer rules due to having to redesign interfaces retrospectively. If websites, apps, platforms and marketplaces were instead designed in a way that ensures compliance with existing legal provisions, for instance by not using dark patterns that are prohibited through the UCPD's general provisions, then such costs would not have been incurred.

It is important to note that the **targeted survey** revealed higher costs to do with adjustment for traders. The largest costs were identified as relating to familiarisation with consumer protection rules and the costs of external services. The respondents to the compliance costs section of the questionnaire were traders and their representative associations. Adjusting business practices relating to changing website design was considered less onerous than other types of costs by respondents. 12.5% considered that these were very low costs although nearly 70% considered these costs to be moderate or significant.

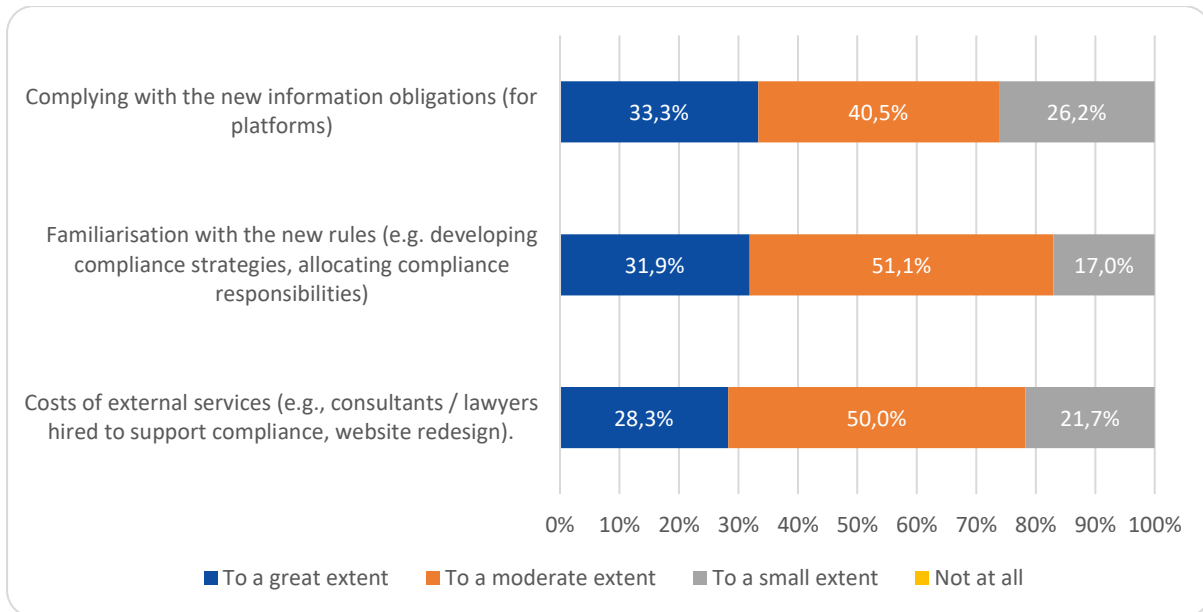
The targeted survey included questions regarding the specific costs of the MD²⁴⁸. The largest costs were perceived to have arisen from one-off costs, such as familiarisation with the new rules followed by the costs of external services to advise on compliance with these rules.

²⁴⁶ This assumes that each employee spends 1.25 hours a day and 40 days in a year per company (for two employees). The average hourly cost in 2022 were estimated by Eurostat at EUR 30.5 per hour.

²⁴⁷ For comparison, the earlier fitness check considered that one-off costs of compliance checks and adjusting business practices concerning advertising and marketing targeted towards both consumers and businesses to range between EUR 1 160 and EUR 8060 per business across the five sectors covered in the study.

²⁴⁸ Q48: to what extent have the regulatory amendments of the MD resulted in new increased costs?

Figure 3.9 – To what extent have the regulatory amendments stemming from the Modernisation Directive’s adoption resulted in new or increased costs in the following areas? (n = 47)



Source: *targeted consultation*

- The most significant costs from the MD relate to the disclosure of ranking criteria (64.8% of respondents thought that these costs were moderate or significant).
- Familiarisation with the new rules – (83.0% of respondents thought that these costs were moderate or significant).
- Costs of external services (78.3% of respondents thought that these costs were moderate or significant).

These relatively high costs can be explained by the fact that the requirements under the MD are relatively new, therefore, there are greater familiarisation costs during this initial application period.

Qualitative insights into the costs are more relevant than the quantitative responses. Some useful qualitative feedback was received through the targeted survey regarding the costs of applying EU consumer law in conjunction with other relevant legislation, such as digital laws and the types of costs incurred in relation to adjustment costs. This is summarised in the next box and highlights the difficulties in providing estimates on the costs but also the **incidence of compliance costs when rules are fragmented**.

Qualitative feedback from targeted consultation on the costs from compliance

One major online platform mentioned that “*the introduction of new obligations such as through the MD or the DSA - necessarily entails mobilising internal and external resources. These are needed to analyse the requirements and their scope of application, to assess their applicability across our various products and services and to identify and roll-out any remediation actions, where deemed necessary. Furthermore, practical aspects such as coding and engineering solutions, translating content or notifying users, add constraints and require careful planning and time for proper implementation*”.

Other large tech sector interviewed also pointed to the complexity of applying new EU legislation that helps to protect consumers, which extends beyond consumer law alone and includes digital and sectoral legislation. For instance, both another major global platform and a large tech player producing devices and running platforms for apps noted that it was often exceptionally complex to ensure compliance with new EU rules, whether this relates to changes through the MD or other legislation strengthening consumer protection, including digital and data laws. The reason was that they are often very large-scale businesses with many different business divisions, providing a high number of different types of services and products to consumers, and therefore checking compliance for each of these involves considerable complexity even if the legal changes themselves are relatively straight forward, such as the strengthening of information disclosure rules through the MD, the DSA and the AVMSD.

A major global online marketplace noted in respect of the targeted consultation that “*It is difficult to answer the questionnaire as one company on behalf of all the business lines*”, which demonstrates the challenge in obtaining compliance costs data from a single company as compliance costs are likely to vary within large firms by business area, given that different legislation is applicable to different products and services.

Further feedback was received on the nature of the costs and whether there were differences between countries in the transposition of EU consumer law and due to gold-plating (going beyond EU rules and introducing further new national rules). A stakeholder commented that:

“Fragmented implementation and interpretation of consumer rules across EU Member States creates unnecessary costs and administration for businesses and potential ambiguity and confusion for consumers. Interpretative guidance goes a way to reducing confusion, but we believe the Commission should continue to work with Member States to ensure a consistent implementation, interpretation and enforcement of the existing consumer rules across Member States”.

Other stakeholders responding to the targeted survey were concerned about the potential scope for further compliance costs were some problematic practices already (implicitly) covered in the Directives to be regulated through more specific rules.

“The EU consumer law acquis already imposes strict rules relating to subscription traps and dark patterns, in particular under the UCPD and CRD (both of which were recently updated in the Omnibus Directive). We therefore suggest that the EC issues clearer guidance regarding the application of existing law to these practices, particularly those considered to be 'dark patterns', rather than issuing further legislation which would require significant additional implementation and interpretation costs”.

3.2.3.1.2 Administrative costs

There are other recurring costs from complying with EU consumer laws, such as checking ongoing compliance with legislation, for instance when launching a new updated interface on a website, app, platform or marketplace, or following the new information disclosure rules under the MD.

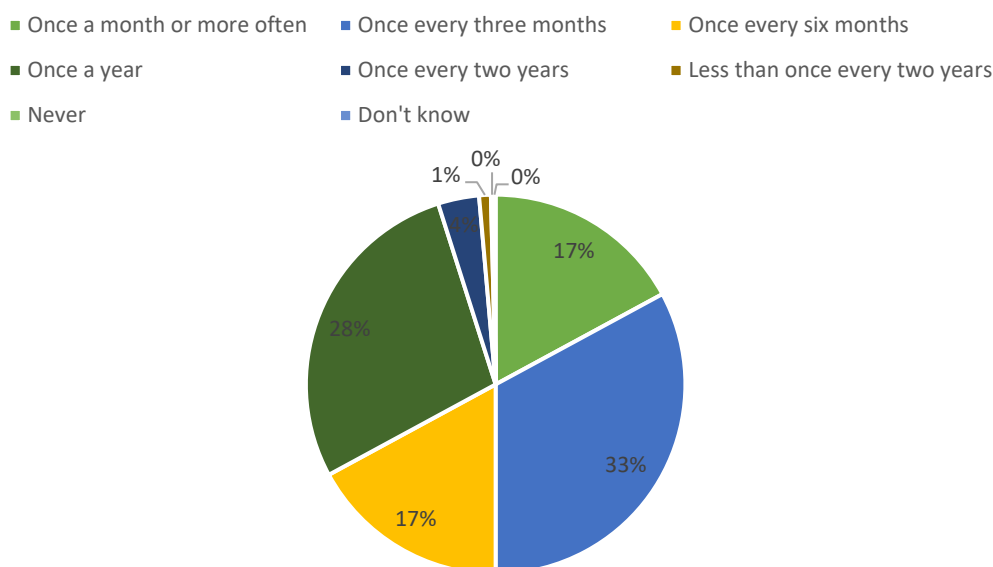
The enterprise survey also asked about any resources required to ensure compliance on an ongoing basis annually. On the issue of **checking compliance with legal requirements to ensure the fairness of digital commercial practices**, 67% of respondents checked at least once every six months that advertising/marketing and standard contract terms for online sales still comply with national legislation. However, 50% also checked more frequently, at least

once every three months. **Yet, 84% of companies reported no costs or low costs.** 15% reported high costs; and 1% did not know.

The enterprise survey also asked about the costs when trading **cross-border** (i.e. considering only on-line sales to consumers in other EU countries²⁴⁹). **Only 11% of traders reported high costs** (which is comparable to online sales in the digital area more generally). It is important to note that the targeted survey noted much higher figures (and when trading cross-border, 80.9% of respondents note that they incurred additional costs to check compliance with the legal requirements of other Member States regarding pre-contractual information, advertising/marketing and standard contract terms²⁵⁰); but the targeted survey was comprised of a majority of traders who operated cross-border, which is likely to explain the differences in perception.

Regarding the frequency of ongoing checks of compliance among traders, the enterprise survey found that 17% of traders checked 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.

Figure 3.10 – Ongoing checks of compliance²⁵¹ (N = 1000)



Source: Enterprise survey, Digital Fairness fitness check study

By country, 25% of companies in Portugal and 24% of companies in Sweden recorded high costs but in Spain, this figure was only 7%. At a sectoral level, the largest proportion of high costs was recorded within *Retail sales of telecommunications equipment in specialised stores* (24%) and *Retail sales of audio and video equipment in specialised stores* (23%). Low costs

²⁴⁹ Q16 asked the costs of checking business compliance considering online sales to consumers in other EU countries. Only 129 out of the total responded to this question. Q14 asked about compliance costs in more general terms (to what extent has compliance with consumer law resulted in costs to your business in the digital area?)

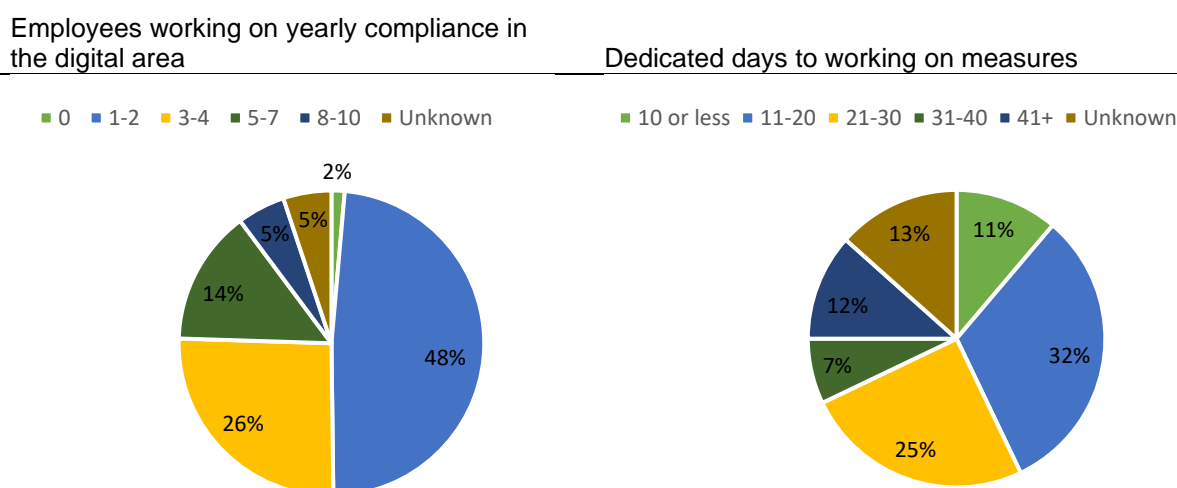
²⁵⁰ Q44: When you entered another EU country's market, did you incur additional costs to check compliance [...]?

²⁵¹ Question - In recent years, how frequently have you checked that your advertising/marketing and standard contract terms for online sales still comply with national legislation?

were most significantly reported by Romanian companies (62%), while 46% of companies in Spain and 48% in the sector *Retail sales of information and communication equipment in specialised stores* recorded no costs relating to this issue.

These compliance checks have resource implications. In terms of the resources **used annually**, the resources dedicated were largely similar to those highlighted under the adjustment costs. On average, **3 employees** are dedicated to this work on an annual basis but in this case the median was **2 employees (and mode is 1)**. The most frequent response by percentage of respondents (32%) was that enterprises dedicated between 11 and 20 days (with 27% of respondent indicating more days than 20). However, given that responses varied across the remaining respondents with some indicating a higher number of days, we have taken the median of 21 days as the benchmark. The average costs of **external services annually were estimated at EUR 2547; but the median is EU 1,800.**

Figure 3.11 – Resources dedicated annually



Source: Enterprise survey, Digital Fairness fitness check study

Based on the number of traders reporting high costs, 15% of the total, and as costs of €1,280 a year (2 employees as reported in the median spending 21 days annually but an hour a day²⁵²), the total administrative costs of checking compliance can be estimated at **EUR 249.8m**. This figure should be read with caution however as it is highly variable to changes in assumptions and larger annual costs of EUR 2,500 by company (based on average costs of external services) could yield compliance costs of around **EUR 487.5m annually**.

Information obligations recorded a large percentage of **no costs** (40% of respondents). Most significantly, the largest proportion of companies in Sweden (50%) and companies in Hungary (43%) noted no costs. Only 10% of respondents indicated that there were high costs. At a sectoral level, 54% of *Retail sale of audio and video equipment in specialised stores* reported no costs from information obligations. The highest costs in this area appear to be concentrated in the *Telecommunications* sector (15%) indicated high costs and *Retail sale of information and communication equipment in specialised stores* (14%) indicated high costs. However, as with other areas, the largest proportion overall recorded low administrative costs relating to the provision of information. The enterprise survey findings differ somewhat from

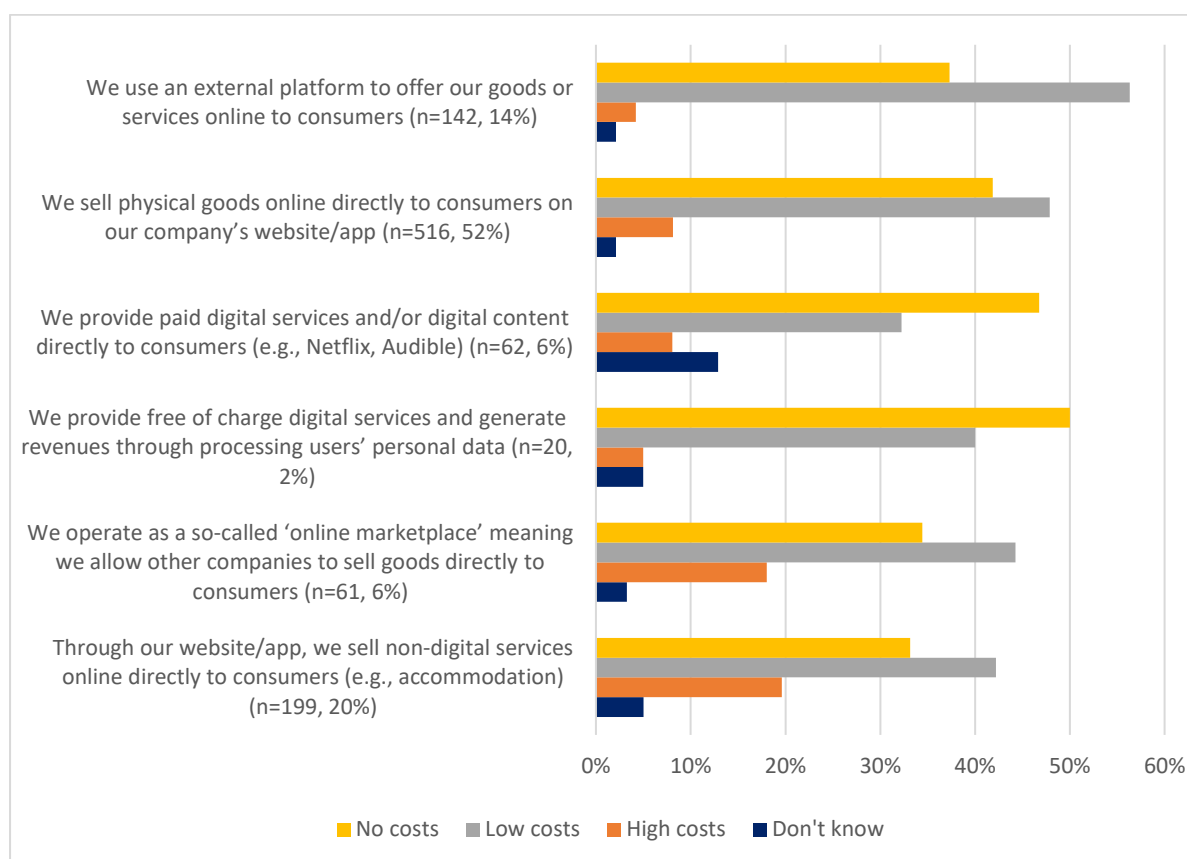
²⁵² An average hourly labour cost in the European Union in 2022 of 30.5 Euros has been used. We have assumed a bit less time in checking compliance per day per employee as they are already familiar with the legislation. Yet, we have err on the side of caution and still assume that this is not far from the amount of time spent on adjusting practices and becoming familiar with the legislation.

the open feedback during interviews and the targeted survey as some traders find pre-contractual information requirements rather burdensome.

These costs have not been estimated for the purposes of this fitness check, except in respect of new obligations introduced through additional transparency disclosures for marketplaces recently introduced through the MD (and any costs from this aspect is expected to be covered by the compliance costs calculated above).

Regarding the costs from information obligations, the results disaggregated by stakeholder type are presented below. Interestingly, there were differing perceptions of the costs of information obligations among different types of enterprises operating in the digital environment. Overall, most respondents perceived there to be either no costs or some costs. For instance, 50% of traders providing free digital services perceived there to be no costs linked to information obligations and a further 40% low costs whereas only 5% stated high costs and 5% do not know. Among traders selling physical goods online to consumers, 42% stated no costs and a further 48% low costs, compared with only 8% high costs and 2% do not know.

Figure 3.12 – Costs from information obligations (N = 1000).

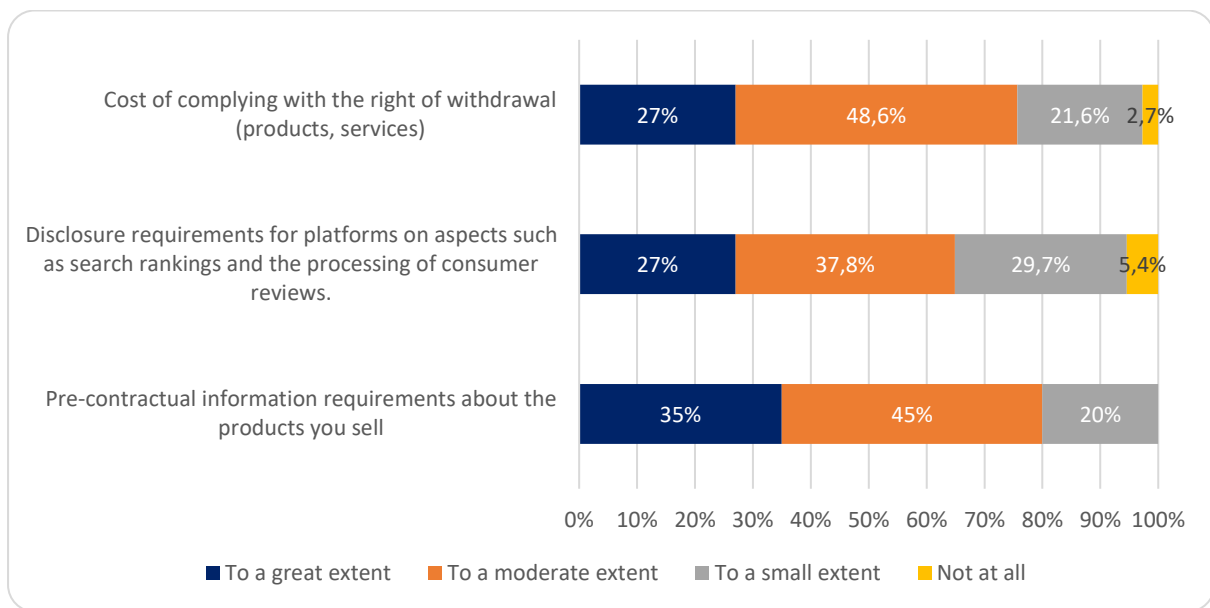


Source: enterprise survey

Regarding traders that perceived there to be high costs, the proportion stating this differed by stakeholder type. Among those operating websites/ apps selling directly online to consumers, 20% perceived the costs of information obligations to be high, compared with 18% of online marketplaces (which are subject to new disclosure requirements under the MD), whereas only 5% of those providing free digital services. Based on interview feedback, this may be because e-commerce traders selling goods online complying with the CRD's pre-contractual information obligations perceived these to be somewhat burdensome.

The targeted survey asked about additional compliance costs from the application of EU consumer law in the digital environment²⁵³ and costs specific to the provision of information²⁵⁴. The following figure shows the results. 35% of respondents agreed that providing pre-contractual information about the products implied additional costs to a great extent, with 45% noting that the costs from this were of moderate extent. Nearly 50% of respondents (48.6%) agreed that the costs of complying with the RoW were moderate. It should be noted that a high percentage of respondents stated “do not know” and these have been taken out of the graphs given the need to assess the responses of those that were able to express a view on costs.

Figure 3.13 – To what extent has compliance with EU consumer law requirements in the digital area resulted in the following additional types of costs relating to information obligations for your business? (n = 40)



Source: targeted survey

The most significant costs from the MD relate to the disclosure of ranking criteria (64.8%% of respondents thought that these costs were significant or moderate). Informing consumers about the processing and verification of consumer reviews was also considered to be of moderate to significant scale²⁵⁵. 25% of respondents however revealed no additional costs from informing consumers about the price being personalised. A 2022 EP study²⁵⁶ on personalised pricing highlighted that there are few incentives to personalise prices in a way that consumers are offered a product at their personally best price, as this could lead to a loss of revenue. The same study noted that the possible costs of personalisation often prevented traders from applying it in practice. Moreover, SMEs may lack sufficient data or have adequate technologies to adapt prices with enough precision. The technology requires additional investments to automate pricing samples while the potential increase in profit margins is rather uncertain. Furthermore, some traders may refrain from price personalisation due to a fear of negative consumers’ reactions.

²⁵³ Q36: To what extent has compliance with EU consumer law requirements in the digital environment resulted in any additional types of general compliance costs for your business?

²⁵⁴ Q38: to what extent has compliance with EU consumer law requirements in the digital area resulted in the additional types of costs relating to information obligations for your business?

²⁵⁵ Q49: [...] please provide an indication of the scale of the increase...

²⁵⁶ IPOL | Policy Department for Economic, Scientific and Quality of Life Policies (2022): [Personalised pricing \(europa.eu\)](https://ec.europa.eu/eipol/en/personalised-pricing)

Few respondents were able to quantify the significance of the volume of compliance costs. The majority indicated 'don't know'. This may explain why 25% of respondents noted no additional costs as personalised pricing practices are still limited (as highlighted in our case study). While a relatively small number answered the question, these included major EU associations and very large traders.

Table 3-7 – Overview of significance of compliance costs according to targeted consultation (N=16)

Stakeholders incurring costs (EU consumer law)	Significant costs (>20%)	Moderate costs (10-20%)	Low costs (5-9.9%)	Very low costs (<5%)	No additional costs
Informing consumers when the offered price is personalised because of automated decision-making	25.0%	33.3%	8.3%	8.3%	25.0%
Adjusting the presentation (branding/packaging) of goods or aligning their composition/characteristics in different Member States, in view of the new provisions concerning "dual quality"	25.0%	41.7%	16.7%		16.7%
Strengthening of the rules applicable to "free" digital services provided against commercial processing of the consumer's personal data (as regards information obligations, the right of withdrawal)	26.7%	33.3%	20.0%	6.7%	13.3%
Enabling consumers to communicate with the trader via e-mail address and telephone number	28.6%	42.9%	7.1%	14.3%	7.1%
Indicating 'prior' price in price reduction announcements	28.6%	35.7%	7.1%	14.3%	14.3%
Disclosure of ranking criteria and paid placements/advertisements when offering consumers the facility to search for products online offered by different traders	30.8%	53.8%			15.4%
Informing consumers about the processing and verification of consumer reviews	30.8%	46.2%	7.7%	15.4%	

As noted above, in this consultation, respondents revealed a higher level of cross-border activity than in the 2017 Fitness check. Although there are obvious benefits of trading cross-border for traders having access to a larger market, there could be costs to traders having to ensure compliance with different pieces of national legislation when these differ. The following

table shows that most respondents saw moderate costs to do with differences in implementation due to regulatory differences. Again, results show how familiarisation is one of the largest costs due to differences in national laws and their implementation. It should be noted that a relatively small number of enterprises responded to this question, so the results should be treated with caution.

Table 3-8 – Cross-border trading and incidence on costs of compliance due to differences in national transposition and implementation²⁵⁷ (N = 31)

Type of costs	To a great extent	To a moderate extent	To a small extent
Information obligations for online sales (e.g. additional national pre-contractual and other information requirements).	23.3%	60.0%	16.7%
Familiarisation with national specific consumer protection rules for online sales and initial compliance planning (e.g. developing compliance strategies, allocating compliance responsibilities)	25.8%	74.2%	
Checking compliance with additional national legal requirements for online sales regarding commercial practices and contract terms (e.g. check website is not unfair by design; ensure that a contract cancellation button exists)	26.7%	66.7%	6.7%
Cost of external services (e.g. consultants / lawyers hired to support compliance process).	33.3%	60.0%	6.7%
Adjusting business practices (e.g. changing a website design where unfair, deceptive practices are identified, using different standard contract terms if considered unfair, etc.)	39.3%	42.9%	17.9%

Some useful qualitative feedback was received through the targeted survey regarding the costs of applying EU consumer law in conjunction with other relevant legislation, such as digital laws and the types of costs incurred in relation to adjustment costs. This is summarised in the next box and highlights the difficulties in providing estimates on the costs but also the incidence of compliance costs when rules are fragmented.

To complement the above feedback from traders, as noted earlier in the literature review under efficiency, the 2017 fitness check also found it impossible to disaggregate compliance costs

²⁵⁷ Q45: 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?

by individual Directive, unless this related to specific compliance checking activities, e.g. compliance of contractual terms before publishing these when going cross-border.

The above highlights the difficulties of estimating with any accuracy the costs for traders; although though interviews some provisions would appear to be more costly than others. For instance, concerning the **RoW for digital content** – a major provider of a marketplace for downloading apps pointed out that during transactional downloads in the digital environment, there is a requirement to inform consumers about their RoW, but then they must waive their right to the RoW to download the digital content and to complete the purchase. Informing people about their rights and then immediately as part of the same transaction asking them to waive these rights was seen as creating a negative perception for the consumer by the major global tech firm interviewed. The trader stated that it is easier and cheaper for them to allow cancellations at any time and to process refunds than it would be to implement the RoW, which was seen as impractical in the era of digital downloads of content. *“Unlike a product which gets returned, digital content may have been partially used but it is very difficult to establish what percentage of the content has been viewed. Therefore, it is often easier to give full refunds to consumers and to leave the transactional process fully automated rather than to investigate and develop the digital technologies as to how much digital content the consumer has used the content before exercising the RoW.”*

This business practice of preferring cancellations to consumers exercising their RoW is also linked to the price points of the content downloaded (e.g. if a typical download cost 0.99 EUR). If a customer services agent picks up the phone to investigate usage of digital content during the period prior to exercising the RoW, there would be much high labour costs than the revenue derived from selling the content – estimated at 30 EUR per call. Full automation is required to make a profit, therefore, processing cancellations which can be made at any time is easier for many traders in digital content and services than allowing RoW requests. This may be an **opportunity for simplification**.

The new requirements under the MD to check the authenticity of online reviews to prevent fake reviews are likely to vary by sector. Some sectors rely more heavily on such reviews to drive digital sales, such as e-commerce websites, tourism websites, especially accommodation booking provides. However, there was limited feedback on the specific costs of checking for online reviews, although this issue was investigated for the IA of the MD and it was found that SMEs would find it burdensome to check whether reviews are genuine, whereas platforms can more readily pay for and use automation software to detect fakes.

EQ6(2) – For those SMEs involved in business on a cross-border basis, were there any additional compliance costs?

The consultations revealed that SMEs responding to the enterprise survey appear to be operating mainly 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 moderate (only 17% indicated high costs), with the highest costs stemming from the familiarisation with the national legislation and initial compliance planning.

The targeted survey respondents were more active on trading cross-border (70% of respondents) and revealed higher costs but the number of SMEs responding was fairly low to extract conclusion. The number of trade associations responding was larger (N=55) and 36% agreed that the costs for SMEs were larger (which is of more significance to traders operating cross-border judged by the activities of respondents).

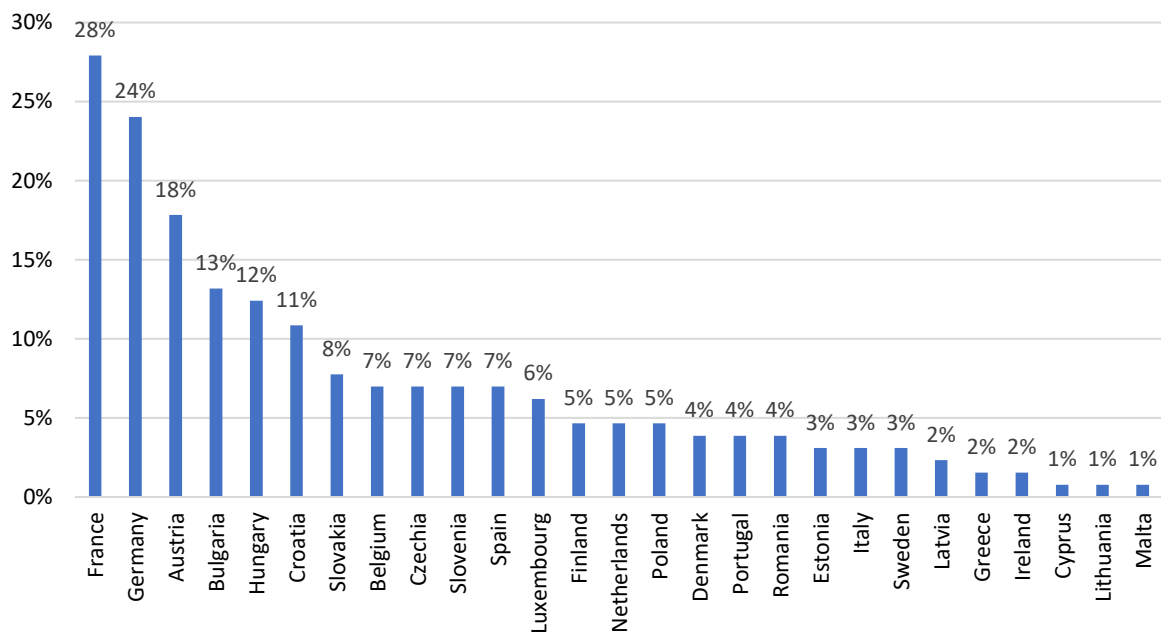
When SMEs were asked about business practices in other EU countries in the enterprise survey²⁵⁸, only 13% of respondents indicated that they had sold or provided products or services online to consumers in other EU countries in the last 12 months. This was greatest

²⁵⁸ Q16.4 Please provide estimates of the additional costs of complying with consumer law when trading cross-border. N=1000

in France, Italy, Poland, Romania and Estonia (all 15%) and, in very small companies (14% in companies 1-5 employees) and very large companies of over 250 employees (14%).

In terms of where companies have indicated they conducted new business, the graph below provides a breakdown, the countries where traders exported most to new markets within the EU-27 were France (28%), Germany (24%) and Austria (18%).

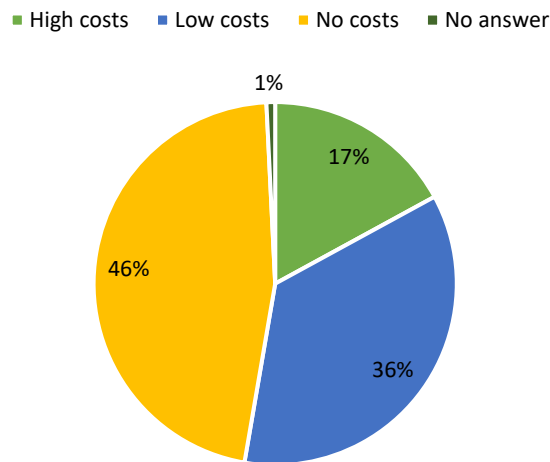
Figure 3.14 – Countries in which companies did business in other EU countries (N = 129)



Source: Enterprise survey, Digital Fairness fitness check study

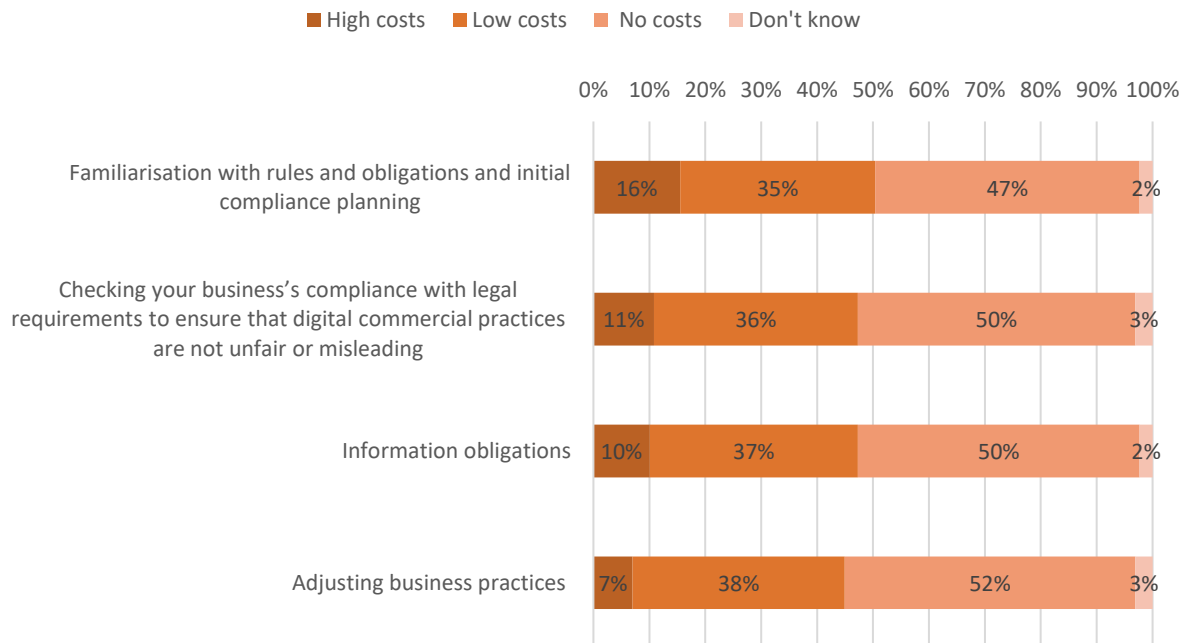
Regarding the costs associated with entering new markets, 17% of respondents experienced high costs. Most companies indicated no costs in response to any compliance issues (see Figure below). Where costs were reported, the greatest issue facing companies was high costs arising from **familiarisation with rules and obligations and initial compliance planning** (16%). **Adjusting business practices** recorded the largest percent of companies indicating no costs.

Figure 3.15 – Costs of compliance checks in new EU countries (N = 129)



Source: Enterprise survey, Digital Fairness fitness check study

Figure 3.16 – Costs by area for online practices (N = 129)



Source: Enterprise survey, Digital Fairness fitness check study

When respondents were questioned about resources they dedicated to compliance when trading cross border, 63% of respondents indicated they dedicated 1-2 employees, 88% indicated 4 or fewer. The average of costs of external services needed to comply with consumer law trading across borders was EUR 1286, but the median was EUR 1,500. This was greatest in Estonia (EUR1623) and Germany (EUR1529), and lowest in Italy (EUR 836). On a sectoral level this was greatest within the *Gas and electricity services* sector (EUR 1561).

Our respondents to the targeted survey agreed that the burden of regulatory compliance is proportionately greater for SMEs than larger traders. Only 13% thought that the costs of regulatory compliance with the three core EU consumer law Directives are similar for SMEs and large traders²⁵⁹. The number of SMEs directly responding to the targeted survey was very small to extract conclusions (only three respondents to this question) but business associations were an additional source of responses on this question (55 business associations responded to the same question) and 36% agreed that the regulatory compliance costs are more costly for SMEs than larger companies. Thus, it will not be unreasonable to suggest that the costs for SMEs are larger than for larger companies, especially regarding those trading cross-border.

3.2.3.1.3 Costs of complying with new digital-specific and information disclosure requirements due to the Modernisation Directive

The focus of the costs for traders was on assessing compliance costs with EU consumer law in the digital environment. However, these rules typically also apply offline due to technology-neutrality and the general principles-based approach (i.e. presently, there are not many digital-rules in EU consumer law in comparison with digital and data EU laws, such as relating to online interface design and consumer choice, specific rules on influencer marketing and transparency etc.

However, some digital-specific requirements have recently been introduced, notably through the regulatory amendments made through the MD to underlying consumer law. In addition, most recently in November 2023, there were various regulatory amendments made to the CRD due to Directive (EU) 2023/2673 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC. This led to rules on the prohibition of dark patterns for financial services in interface design and the introduction of a right of withdrawal button. Some of the new rules through the MD and the revision of the DMFSD are digital-specific. A list of examples of digital-specific rules now present in EU consumer law is presented below:

New digital-related information disclosures in the MD:

These disclosures are for platforms (and in some instances also marketplaces):

- Transparency of search rankings.
- Informing consumers that a price has been personalised based on profiling.
- Inform whether the third party offering the goods, services or digital content through the online marketplace is a trader or not. If the third party is not a trader, inform that the consumer rights stemming from consumer protection law do not apply to the contract.
- Inform consumers whether online reviews have been authenticated.

Other digital-focused consumer rights

- Extending the right of withdrawal to data-paid services. Applying consumer protection rights to contracts for the provision of digital content or digital services without the consumer paying a specific monetary amount, but in exchange for their personal data.
- Specifying exceptions to the right of withdrawal if the consumer has already used digital content.

Digital-related requirements in the CRD due to integrating regulatory amendments

- Prohibition of dark patterns for financial services in interface design and the introduction of a right of withdrawal button.

²⁵⁹ Q52: To what extent do the costs [...] differ between SMEs and large businesses?

See Part 2 of this study for more details on the MD changes that are digital-relevant and the coherence section for details on the DMFSD revision.

It was not possible to quantify the costs of each of these new changes. As mentioned earlier, traders find it difficult to isolate the costs of specific Directives, and in respect of specific provisions.

The information cost relating to the new transparency obligations for platforms is very minor as often, there is simply a requirement to inform a consumer about something such as personalisation through price automation. Providing this information usually only requires putting a pop-up box on a platform to ensure that consumers are informed upfront. However, there are wider associated compliance costs linked to introducing new information requirements that are less concerned about the information itself, and relate to managing compliance more generally. For example, informing consumers that a price has been personalised is not technically difficult, but will require wider compliance costs than the information itself, already considered under general compliance costs and adjustment costs, such as legal services (in-house and/ or external legal counsel on the implications of proposed changes for platforms). Platforms are complex businesses often with many different business divisions so they will consider the implications of any regulatory changes including information provisions across their business divisions. There are then adjustment costs such as the costs of platform developers to make the necessary changes to the design interface which requires reprogramming. Therefore, the information itself is not costly to provide but the ancillary steps needed to apply the new requirements by a platform will cost them money beyond information provision alone.

Similarly, providing information that reviews are checked to ensure they are genuine means only providing some basic text for a website page, with a negligible cost. However, the process of actually checking whether reviews are fake requires platforms to put in place procedures and processes to automatically check the authenticity of reviews (with some additional manual checking to ensure the robustness of the automated detection). This has led to costs for platforms. However, survey respondents were not generally able to quantify the costs of information provision. Rather, they estimated these costs to be low in the case of the targeted survey, and moderate in the case of the enterprise survey.

Concerning the new information requirement on **price reductions in the Price Indication Directive**, which will require traders – both online and offline traders – to provide information regarding the average price in the previous 30 days to calculate a reference price to compare with the promotional price, thereby ensuring transparency. This is a good example that there may be markedly different informational cost implications between online and offline traders. For instance:

- **Online marketplace and large e-retailers selling products** – the cost of information provision is estimated to be low due to the marginal costs involved. Given the frequency of price changes on many e-commerce websites, such a trader would need to invest in reprogramming their pricing algorithms, such that an average price over 30 days can be automatically calculated. Whilst this would require several days programming and could cost 2,000 – 3,000 EUR, once performed, it could be applied across a very large number of products and therefore the average cost per product after such one-off costs would be negligible in terms of ongoing costs.
- **Conversely, offline retailers in some product sectors have a high frequency of price changes but need to calculate an average reference price manually** (e.g. food retail, retailers of clothing, textiles and shoes). In such sectors, it is relatively common practice to engage in price promotions multiple times per month. This is labour-intensive and whilst it may take little time for each individual product, as independent retailers may sell hundreds of products, the compliance costs are

potentially more significant. There were found to be methodological difficulties in manually calculating an average reference price in sectors where prices change frequently, which may make it time-consuming and burdensome for SMEs. However, there are trade-offs, given the benefits for consumers of having transparency that the prices shown are genuine promotions.

Regarding the perceived impact among marketplaces due to the introduction of information disclosure requirements for marketplaces, in the targeted survey, complying with new obligations was seen as having resulted in new or increased costs by 33.3% to a great extent, 40.5% to a moderate extent and 26.2% to a small extent (N – 47). The disclosures themselves and designing these into platforms, apps and websites were not seen as that costly. New disclosure rules under the MD require platforms and marketplaces to update their design interfaces to provide pre-contractual information to consumers, for instance integrating a pop-up box to inform a consumer that pricing has been personalised, or specifying the general criteria used in search rankings. Large traders instead pointed to the cumulative costs of complying with consumer law in conjunction with other EU legislation.

Other digital-specific compliance costs were too early to assess, such as the DMFSD revision through regulatory amendments to the CRD, which was only published in November 2023. This has led, for instance, to the incorporation of a requirement in the CRD for all traders to design in a withdrawal button onto their website or interface such that consumers can exit from a contract as easily as they entered it. If the body of EU consumer law were to follow the general trajectory of other areas of EU law, such as digital law and data law and become more specific in terms of digital requirements, then future fitness checks could quantify the digital-specific compliance requirements in more detail. However, traders often provided qualitative feedback on the impact of changes and were not able to quantify these.

3.2.3.2 Benefits to traders

EQ6(3) – What are the main expected benefits of consumer law Directives? How far have these actually been manifested in practice? (traders)

The main benefits to traders include reducing regulatory uncertainty about the legislation particularly when trading cross-border and the online sale of physical products and services and to a lesser extent the online sale of digital content and services.

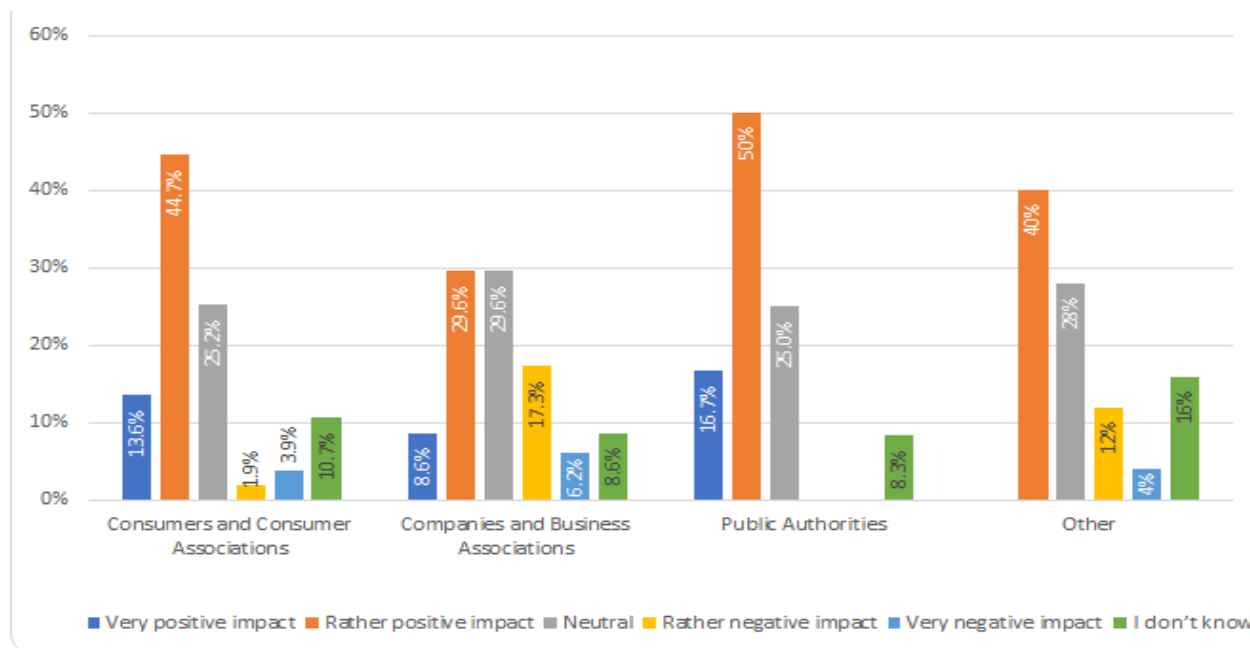
This facilitated e-commerce by harmonising the rules and thus increased the possibilities to trade outside the country of origin, although trade is still conducted mostly within the same country.

Indirect benefits arise from the increased volume of e-commerce due to increased consumers' trust; but it is not possible to calculate an attributable fraction.

Businesses/trade associations responding to the public consultation and targeted survey identified positive effects from EU consumer law, such as regulatory certainty and reduced regulatory fragmentation through fostering the Digital Single Market.

In relation to the public consultation findings, respondents were positive about the benefits of applying EU consumer law in the digital environment in fostering a level playing field amongst businesses addressing consumers in the EU.

Figure 3.17 – Views on impacts from existing consumer law framework on a level playing field among businesses addressing consumers in the EU (N = 221)



Source: public consultation survey

Among traders and their representative associations, for instance, 8.6% stated that EU consumer law has had a very positive impact, 29.6% a rather positive impact and the same proportion a neutral impact. 17.3% perceived it has had a negative impact and 6.2% a very negative impact.

According to a large percentage of respondents to the targeted survey²⁶⁰, EU consumer law Directives have provided regulatory certainty to businesses when trading online and cross-border to either a significant or to a moderate extent. In particular:

- 54.7% believe that they have brought regulatory certainty when trading online cross-border/in another Member State to a moderate extent and a further 20.5% to a great extent; and
- 50.4% believe that they have brought certainty when trading online within their Member State and a further 32.8% to a great extent.

The targeted consultation also showed (see chart on following page) that a large majority of respondents agreed that the rules have facilitated e-commerce through more uniform rules, including by harmonising rules on the right to cancel online purchases within 14 days (86.2%) information requirements in distance contracts (86.4%) and unfair commercial practices (84.2%). Furthermore, the Directives were viewed as having contributed to the functioning of the EU digital single market (87.1%) to a great and/or moderate extent. The Directives were viewed as having contributed least (% of respondents indicating 'not at all' as the effect) to ensuring clarity and fairness regarding the marketing of virtual items and intermediate currencies (19.1%), personalisation practices (14.2%) and preventing dark patterns (13.6%).

Businesses will also benefit indirectly from increased consumer confidence, with will result in an increased number of transactions in domestic markets but also cross-border. The 2017 fitness check did not provide an estimate of the benefits to traders although it did acknowledge

²⁶⁰ Q12: overall, to what extent have the EU consumer law Directives provided regulatory certainty in the digital environment?

that traders operating cross-border were the ones reaping the most tangible benefits from the harmonised rules. The public consultation showed the following:

- 40% of all respondents (n=221) thought that the existing framework has had a positive or very positive impacts on the increase in e-commerce across EU Member States.
- 25% of companies and business associations (N=81) considered that it had increased commerce across EU Member States and 23% within their own country.

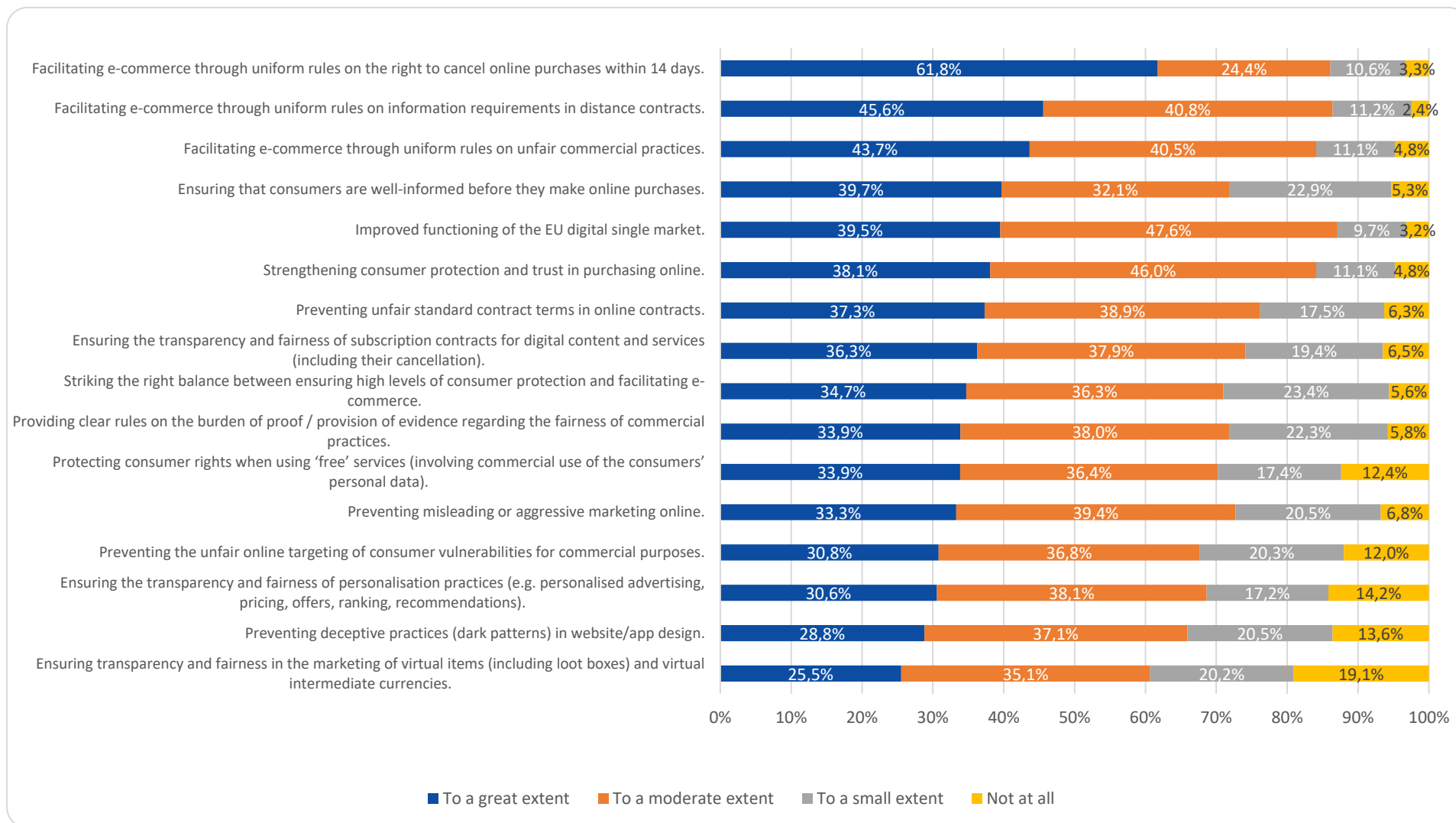
The enterprise survey shared similar conclusions and showed that the largest positive impact is mostly related to strengthened trust among consumers in making purchases of goods, services or digital content online (87% of respondents; N=1,000). This was followed by:

- 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%).

In 2022, the European B2C e-commerce turnover increased from €849 billion in 2021 to €899 billion in 2022²⁶¹. It is reasonable to suggest that part of this increase may be due to more harmonised rules across channels and reduced uncertainty in legislation; but it is difficult to estimate an attributable fraction.

²⁶¹ [European e-commerce continues to grow despite shifting economic environment - EuroCommerce](#)

Figure 3.18 – To what extent have the EU consumer law Directives contributed towards achieving the following benefits? (n=134)



Turning to **feedback from traders and their representatives during interviews**, the EU consumer law framework was generally seen positively as regards the benefit of providing regulatory stability, a pre-condition for Europe's economic competitiveness and individual traders' prospects. However, as detailed in greater detail in a later EQ under relevance and fitness for purpose, the cumulative regulatory changes not only under EU consumer legislation (i.e. regulatory amendments due to the MD), but also under parallel digitally-focused legislation and data protection legislation means that whilst the core applicable legislation has delivered stability, there is a perception among some traders of increased risks that EU consumer law may need to be updated to reflect broader legal developments.

Some large traders and platforms expressed concerns that even when Directives are meant to be maximum harmonisation, there may not always be such harmonisation in practice due to divergent interpretation of the law. This was attributed to the fact that the legislation remains principle-based and therefore does not stipulate in detail which practices are banned especially when there are grey areas, with some elements of a practice prohibited but others not (or where there is a lack of legal definition e.g. of dark patterns). Therefore, this was seen as a risk that could potentially undermine the widely-acknowledged single market benefits. A major global online marketplace with significant operations in Europe noted that the main benefits of EU consumer law were providing a consumer protection framework in which the single market could be fostered.

Whilst the e-commerce market Europe has undergone significant growth in the past 10 years, the drivers were not seen as primarily regulatory by the marketplace. Trends such as digitalisation, accelerated by the pandemic, and faster and more widely available broadband internet connections have made the main difference. Nonetheless, the market could not have grown to the same extent without EU consumer law being part of the enabling pre-conditions.

3.2.3.3 Validation of findings based on the review of previous literature - findings on the costs of compliance and benefits for traders

This section compares our findings with other secondary data for validation.

The previous 2017 fitness check involved 283 enterprise interviews in 28 MS (e.g. 10 per MS). As explained in the section on challenges in assessing costs and benefits, the focus was on the costs of adapting business practices to adjust to national rules when entering new markets, but without a disaggregation by Directive or a distinction between national rules due to EU consumer and marketing and sectoral laws, and purely national rules. This method reflected the fact that often businesses cannot distinguish between the two, as they are typically aware about national rules but not whether these emanate from EU laws or not. Other main findings from the 2017 fitness check's assessment of costs (and commentary on relevance for the present study) were:

Businesses perceived there to be higher compliance costs of doing business cross-border compared with selling these domestically²⁶². However, there was a lack of detailed explanation as to the source of these additional costs e.g. whether these were driven by regulatory fragmentation in national consumer rules due to gold-plating (which in theory should only be possible under the UCTD given the other two Directives are maximum harmonisation), other types of rules or were due to divergent application of EU rules as transposed into national laws. This finding confirms our findings in the targeted survey, although the sample size of this latter survey was rather small and related to companies trading cross-border.

The total costs incurred by all businesses in the EU-28 in the five selected sectors for checking that their advertising/ marketing and standard contract terms comply with national legislation

²⁶² It should not be overlooked that compliance costs with EU laws on unfair, misleading and / or aggressive practices (UCPD), unfair contract terms (UCTD) and on distance contracts (CRD) are applicable irrespective of whether a particular firm sells cross-border or not.

and adjusting business practices if needed amount to **EUR 278 million / year for an estimated 962,261 businesses** in the five selected sectors. Compliance costs were then aggregated across several different types of EU and national laws and do not only focus on EU consumer law. Whilst data was gathered at a sectoral level, estimated compliance costs cover five sectors, but without the disaggregation of compliance costs by Directive or between EU and national laws and regardless of shopping channel²⁶³.

Whilst this data provides a useful benchmark, it can be noted that: (1) the EUR 278 million / year covers five sectors only and was not extrapolated to the European economy as a whole i.e. to all sectors and (2) it covers sectoral laws not only consumer law, therefore should be treated with caution in terms of its utility for the present study. The figures do, however, compare well with the costs of adjustment calculations provided in this fitness check and ranging from **EUR 208m to EUR 303m, but involving a larger number of business trading online (c. 1.3m)**. The number of businesses trading online is comparable to earlier estimates provided in the IA on the online and other distance sales of goods²⁶⁴, but would suggest that the costs per company have decreased since the earlier assessment (which is not unreasonable due to the rapid growth of e-commerce, knowledge transfer and other economies of scale).

Some relevant costs data was obtained through the **Impact Assessment Study of the CRD** regarding the anticipated costs for traders of complying with the CRD.²⁶⁵ The focus in the IA study on the CRD was on assessing the costs of regulatory fragmentation and the benefits of adopting a maximum harmonisation Directive. Although the costs appear to be bigger than the costs used under this fitness check, they also confirm the findings that the costs for business operating cross-border are larger. Yet, these were offset by the benefits from reduced fragmentation. Moreover, the impact assessment concluded that there was limited available data do not allow definitive conclusions about the level of costs faced by businesses in ensuring compliance with the Directive (in CEC, 2018; page 29²⁶⁶). It is only reasonable to expect that the MD has further reduced the compliance costs by, e.g. extending the scope of the CRD to "free" digital services but costs could have equally decreased over time as traders become familiar with the rules.

Estimated administrative costs from the CRD Impact Assessment

The estimated administrative costs imposed by EU consumer law to businesses selling only domestically is 5526 Euro for distance sellers and 6625 Euro for direct sellers.

The estimated one-off costs per company for distance sellers of trading only domestically were EUR 5526, EUR 9276 for traders trading cross-border in 1 or 2 additional MS and EUR 15,526 for those in 3-5 additional MS. The estimated administrative costs for a business wanting to sell in all 27 Member States are EUR 70526 for distance sellers.

However, these costs were offset by benefits, such as the reduced costs of regulatory fragmentation through avoiding different national rules, which were seen as "a heavy burden on business".

Source: IMPACT ASSESSMENT REPORT on the CRD (2008). See pg. 12 and Annex 7.

The **impact assessment of the MD** was a useful data source. It is easier to capture the MD's one-off costs as these only came into effect from May 2022, whereas the other Directives

²⁶³ Source: 2017 Fitness Check, pg. 54 of the SWD.

²⁶⁴ For comparison, in 2017 it was estimated that there were 930,000 business were selling online domestically and 400,000 businesses were selling on-line cross-border (source: CEC (2017): Commission Staff Working Document on the Impacts of fully harmonised rules on contracts for the sales of goods supplementing the impact assessment accompanying the proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods

²⁶⁵ COM(2008) 614 final, COMMISSION STAFF WORKING DOCUMENT accompanying the Proposal for a DIRECTIVE on consumer rights, IMPACT ASSESSMENT REPORT

²⁶⁶ Commission Staff Working Document Impact Assessment. SWD(2018) 96 final PART 2/3

within scope date from 1993, 2005 and 2011 respectively (the CRD entering into force from 2014). As the IA study was carried out in 2018, this used a more standardised format for setting out the costs/ benefits linked to the policy options. Some policy options quantified related to digital-only measures. The study concluded that EU consumer legislation is not considered burdensome compared to other areas of legislation²⁶⁷. An analysis is provided in the IA of the direct costs of changes to be made through the MD. This includes several digital-specific proposed changes. It was observed that there would be some initial familiarisation costs for traders, for instance due to:

Strengthened disclosure requirements for online marketplaces to improve transparency for consumers. This would also require initial familiarisation costs, followed by minor costs for traders to provide the information. An example was the new requirement to inform consumers when making a transaction whether the trader using their marketplace is an individual seller or a (professional) trader. SMEs estimated one-off costs of EUR 2,179 on average (median: EUR 50) and annual regular/running costs of EUR 3,887 (median: zero). However, large firms only provided qualitative feedback on costs. The costs per firm are of a similar order of magnitude of those considered in this fitness check.

Extending the CRD to cover “free” digital services. Regarding potential annual costs, in the SME panel, SMEs estimated on average EUR 8 367 (median: EUR 33) for new pre-contractual information requirements and EUR 9,119 (median EUR 50) for the right of withdrawal. A very significant difference between the average and median costs can be noted highlighting the high variation in responses to make the average meaningful.

Regarding the **benefits of taking action to strengthen the EU consumer law framework for traders**, a benefit identified in the IA study was being able to eliminate unnecessary costs for compliant traders. Some examples of benefits were quantified for traders specific to regulatory changes affecting traders in the digital environment:

Lack of transparency and legal certainty for B2C transactions in online marketplaces. There would be certain benefits depending on the specific information disclosure due to specific transparency requirements for contracts concluded via online marketplaces. Examples were the requirement for marketplaces to inform consumers whether the trader is an individual or a professional. It was concluded that transparency requirements should reduce costs for online marketplaces as should problems arise, they would not need to clarify the status of the trader to consumers. If consumers already know who their contractual partner is, they would know who to contact in case of a problem, so there should be fewer queries to be handled by online marketplaces. SMEs in the SME panel consultation anticipated on average one-off savings of EUR 214, with annual savings of EUR 391.

Extending the CRD’s RoW to cover “free” digital services. Replies to the targeted consultations indicate that traders already face unnecessary costs linked to the need to check and comply with national rules on precontractual information and the right of withdrawal for “free” digital services. At least three Member States had already regulated “free” digital services with more considering doing so at the time. This had led to regulatory fragmentation and additional costs.

Regarding the expected benefits, by providing a clearer legal framework for “free” digital services across the EU, traders would benefit from reduced costs related to diverging or uncertain information requirements and incoherent rules for digital content products. This was found to help alleviate barriers to online cross-border trade, such as differences in national contract law (38.1%) and national consumer protection law (37.4%). It would reduce unnecessary costs for compliant traders of checking and complying with possible national rules on precontractual information and the right of withdrawal for “free” digital services. These

²⁶⁷ Commission Staff Working Document Impact Assessment, SWD/2018/096 final - 2018/089 (COD) [EUR-Lex - 52018SC0096 - EN - EUR-Lex \(europa.eu\)](#)

costs were considered disproportionately burdensome by 7 out of 10 business associations in the public consultation. However, consumer associations responding through position papers made clear they supported this change to enlarge consumer rights beyond products, given the relevance of being able to apply the RoW in all digital markets and services.

There would be savings for cross-border traders, due to more legal certainty and harmonised rules. In the SME panel, SMEs expected annual savings of EUR 622 and EUR 396 on average, for pre-contractual information and right of withdrawal respectively.

The impact assessment to the MD²⁶⁸ concluded that the further harmonisation of certain aspects of EU consumer law would lead to savings for cross-border traders due to increased legal certainty and more uniform rules. For example, regarding the harmonisation of UCPD remedies, SMEs indicated one-off savings of EUR 1 405 on average (median: zero) and annual savings of up to EUR 10 000 (average: EUR 704, median: zero). The four responding large companies estimated one-off savings of maximum EUR 1 682 (average EUR 250). The IA to the new Sales and Guarantees Directive, conducted in 2017, concluded that the total benefits from contract law-cost savings due to increased cross-border sales, for retailers who already sell online cross-border, could reach EUR 10.8 bn.

Qualitative feedback regarding the **costs of non-action** in addressing certain problems in the application of EU consumer law, such as ongoing high levels of consumer detriment are referenced. For instance, both the CRD evaluation and the fitness check noted that EU consumer laws have reduced costs for businesses offering products and services cross-border compared with divergent national regulations these replaced.

Overall, the review of previous literature on the costs of compliance for traders with EU consumer law has found that:

There are several **limitations in relying on previous studies for cost-benefit data of the costs of compliance with EU consumer law**.

- Directive-specific costs of compliance are often unavailable, except for the CRD;
- Absence of estimates of compliance costs with EU consumer law in the digital environment, as these have not previously been assessed.

Some **useful data was still obtained through the fitness check 2017²⁶⁹**, and **two impact assessments**. However, there are also some limitations in the utility of this data explained in the previous sub-section on challenges, as not all policy options that were subsequently adopted in the MD were quantified.

In conclusion, previous evaluations and IA studies provide some useful data on the costs and benefits of legislative changes, some of which are relevant to the digital environment (e.g. digital-specific regulatory amendments made through the MD and digital sales in relation to distance contracts within the CRD). However, only limited costs data is available and the MD IA study covers the regulatory amendments made to the UCTD, UCPD and CRD and not the wider set of requirements in the original legislation. Whilst previous studies have been reviewed, due to the lack of comprehensive baseline data and issues around data comparability given the current study's objectives, we have instead mainly relied on primary data gathered through the enterprise and targeted surveys when considering the costs and benefits for traders, complemented by interviews. Overall, the findings are mostly aligned,

²⁶⁸ [EUR-Lex - 52018SC0096 - EN - EUR-Lex \(europa.eu\)](#)

²⁶⁹ Fitness Check of EU Consumer Law, European Commission's DG JUST (2017), study by Civic Consulting. Regarding the methodology for the 2017 fitness check, cost-benefit data was gathered through enterprise interviews. 282 enterprises were interviewed in large household appliances, electronic and ICT products, gas and electricity services, telecommunication services, and pre-packaged food and detergents. Of the enterprises interviewed, only 28% sold cross-border, whereas 72% focussed on their domestic market.

regard to the costs per company of adjustment and checking compliance. Mostly, costs would not appear to be significant.

3.2.4 Costs and benefits for consumers

Consumers have benefited from increased consumer protection, including because of the recent regulatory amendments through the MD.

Trust has also increased in online shopping channels, as evidenced by the Consumer Conditions Scoreboard data 2023 in comparison to previous CCS data.

Additional information disclosures have also allowed them to make more informed decisions. Consumers have benefited from various new digital products and services as well as the improved opportunities concerning ecommerce, allowing them to buy at a more competitive price, which has increased consumer welfare.

However, problematic practices relating to transactions in the digital environment remain both relating to practices already prohibited in EU consumer law, due to trader non-compliance in some instances, and due to the ongoing challenge of strengthening enforcement. This means that consumers still continue to experience consumer detriment in relation to illegal practices and practices that may represent grey areas, in that traders claim they are compliant, but consumers still face non-financial harm, such as having their time wasted. Therefore, despite progress in extending the consumer law framework to include some digital-specific provisions through the MD, outstanding problematic practices documented in the case studies and in the problematic practices section within effectiveness continue to cause consumer detriment.

The consumer detriment has been estimated at between **EUR 6.1bn and EUR 10.7 bn**, which is a conservative estimate that is likely to underestimate the degree of problems consumer face. It is difficult to establish causality with regards to any specific legal gaps in the existing regulatory framework and consumer detriment, as the degree of detriment is also impacted by lack of consumer education and awareness and lack of compliance by traders.

3.2.4.1 Costs for consumers

EQ6(3) – What are the costs to consumers and drivers of costs under the current legislative framework (consumer detriment)?

Unlike for traders, there are no direct costs for consumers of applying EU consumer legislation. On the contrary, there ought to be significant benefits through a reduction in consumer detriment in theory from increased consumer protection. However, in practice, consumers are affected if the legal framework remains ineffective and problematic practices persist, e.g. dark patterns or subscription traps, and if non-compliance by traders and/ or a lack of enforcement remains a problem.

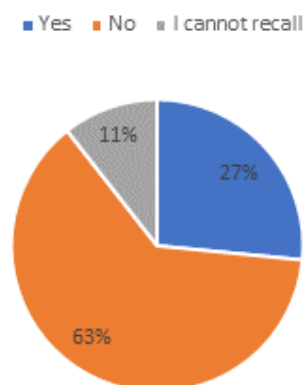
There were two aspects to the methodology. Firstly, we assessed how frequently consumers perceive they have been subject to problematic practices that have undermined their rights and whether this has led to any consumer detriment across problematic practices overall by using data from the consumer survey and from the public consultation. Secondly, we performed a literature review to assess detriment at the level of different types of problematic practices.

Due to the lack of suitable benchmark data pertaining to consumer detriment in the digital environment and the relationship with EU consumer law, primary data collected through the consumer survey and public consultation survey undertaken through this fitness check were the main data sources. The consumer survey of 10,000 respondents revealed that:

27% of consumers (approximately 1 in 3 consumers surveyed) buying online have experienced situations that have caused them **financial loss, time loss or emotional distress** (out of 10,000 respondents).

Figure 3.19 – Problems experienced that caused financial loss, time loss or emotional distress (n = 10000)²⁷⁰

The highest level of consumer detriment in the consumer survey was amongst younger age groups in the sample; 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+. 48% of consumers who engage in gambling activities daily have experienced these kinds of issues, this is in comparison to 37% who engage with these activities several times a week and 20% of those who never engage in gambling activities. Furthermore, 42% of consumers whose daily activities are ‘severely limited’ due to a health problem indicated experiencing these issues, this is in comparison to 31% of those who are ‘somewhat limited’ and 21% of those who have no health-related limitations.

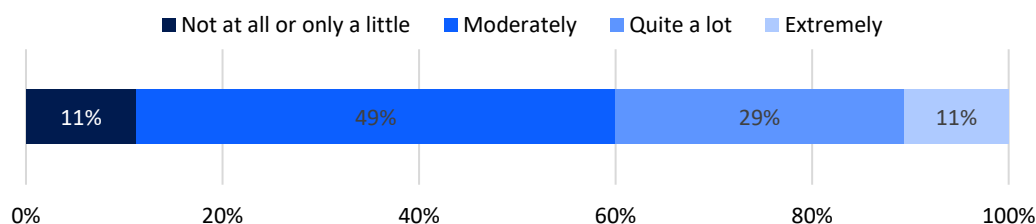


Similar figures were present in the public consultation showed, with over 50% of consumers experiencing problems online up to three times a year and approximately one-third experienced detriment. The full set of response options is considered in the stakeholder consultation annex.

In the consumer survey, of these 27% experiencing problems, **58% of respondents 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**

Approximately half of the respondents mentioned 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 cohorts; 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%).

Figure 3.20 – Distress because of the problem (n = 2657)



Source: consumer survey

The consumer survey also asked about consumer detriment and costs implications. Using the median, two values for consumer detriment have been calculated (refer to methodological annex for more detail):

²⁷⁰ Source – consumer survey, DIGIFAIR study, 2023

- 1- A cost of detriment, **pre-redress**, that includes extra charges and costs of repairs: estimated at **EUR 65**;
- 2- A cost of detriment, **post-redress**, that includes all costs (inc. costs of dispute resolution and expert advice but also the reimbursement) estimated at **EUR 115**.

There are a few studies providing monetary estimates of consumer detriment although fewer are specific to the digital environment. For example:

In **Germany**, 40% of online shoppers experience problems and the financial detriment per capita is estimated at EUR 79.7, for those online shoppers experiencing problems (average post-redress detriment²⁷¹); in **Italy**, 47% of online shoppers experiencing problems. The consumer detriment for those experiencing problems is EUR 52.5 (average post-redress detriment).

These figures from EU MS were broadly similar to those in recent comparator studies from third countries. A 2022 study in the **UK** for BEIS on consumer protection²⁷² researched the extent of consumer detriment. It found that on average, consumers experienced four problems per year, each of which caused EUR 30 (£28) of estimated detriment or a total of EUR 120 / consumer/ annum. A recent OECD study on the financial detriment experienced by consumers reports on post-redress detriment.²⁷³

Another point of comparison can be taken from the Commission's 2017 study on measuring consumer detriment, which examined six markets (mobile telephone services; clothing, footwear and bags; train services; large household appliances; electricity services; and loans, credit and credit cards) in France, Italy, Poland and the UK. These estimates refer to the sum of total post-redress financial detriment and monetised time loss although it is not limited to e-commerce and include other channel shopping. The findings are presented below.

Values for consumer detriment in the European Union by type of product and service (2017 study)

Mobile telephone services: the average detriment based on the 'fair price' approach is **EUR 39.8**, and the average pre-redress and post-redress financial detriment in that market are EUR 64.8 and EUR 55.8 respectively;

Clothing, footwear and bags: the average detriment based on the 'fair price' approach is **EUR 33.8**, and the average pre-redress and post-redress financial detriment in that market are **EUR 49.9** and EUR 25.1 respectively;

Train services: the average detriment based on the 'fair price' approach is **EUR 29.7**, and the average pre-redress and post-redress financial detriment in that market are EUR 64.5 and EUR 46.9 respectively;

Large household appliances: The average detriment based on the 'fair price' approach is **EUR 227.9** for those who experienced a problem with large household appliances while the average pre-redress and post-redress financial detriment in that market are EUR 302.7 and EUR 167.5 respectively;

Electricity services: the average detriment based on the 'fair price' approach is **EUR 152.0**, and the average pre-redress and post-redress financial detriment in that market are EUR 131.9 and EUR 116.4 respectively

²⁷¹ Note that this includes financial detriment due to time loss.

²⁷² Consumer Protection Study 2022: Understanding the impacts and resolution of consumer problems

BEIS Research Paper Number 2022/005. The value includes the initial cost of the product, the cost bared by the consumer for replacing or fixing the product, and other direct and indirect costs (including the loss of earnings and not being able to use another product the consumer paid for, such as not being able to use a hotel booking due to problems with the flight) but also the value of their time and the compensation they may have received.

²⁷³ OECD (2022), Measuring Financial Consumer Detriment in E-commerce, Page 114. The study included an online consumer survey to measure financial consumer harm in e-commerce, which was implemented in February and June 2021 in 13 countries: Australia, Canada, Chile, Germany, Israel, Italy, Japan, Korea, Mexico, Norway, Singapore, Türkiye, and the United States.

The 'fair price' approach is used as a proxy to measure consumer detriment, by subtracting the 'fair price' ('What is the most you would now pay for this [good or service] taking into account all the trouble you had as a result of the problem, including any financial loss, time loss, and emotional stress?') from the price actually paid for the good or service.

Source: CIVIC (2017)²⁷⁴

In 2020, another study for the European Commission also reported a cost of more than EUR 50 to consumers experiencing a scam or fraud²⁷⁵, mostly from online shopping but also from telephone calls. An older study on consumer detriment in Ireland reported values from EUR 8 in groceries to EUR 570 in household goods and services (Ipsos Ireland, 2014)²⁷⁶.

Overall consumer detriment under current legislation²⁷⁷.

Consultations have shown some divergences in terms of the number of consumers suffering consumer detriment, ranging from 27% in the consumer survey to 50% in the public consultation. However, only 214 consumers responded to the public consultation, as well as 10 consumers organisations. However, we have taken an estimate of **30% of consumers experiencing consumers detriment**²⁷⁸ as the sample of consumers in the consumer survey was significantly larger (10,000). Other consumer market monitoring data for 2020²⁷⁹ report similar estimates of consumers experiencing financial loss but with variation depending on market and ranging from 25% to 44% (clothing and footwear and electricity services respectively). On the other hand, the percentages of consumers experiencing non-financial impacts, such as loss of time, anger, frustration, stress and anxiety, are significantly larger, ranging from 68% to 80% (for clothing and footwear and insurance and gas services respectively).

The consumer survey has also provided a significant variation in responses concerning consumer detriment to produce robust conclusions (with average values and median values being far apart). This is, however, not a surprise, owing to the variety of products and sectors being considered. A **lower value of EUR 65** is taken for consumer detriment which includes both financial and non-financial detriment, based on the median values obtained from the consumer survey (pre-redress).

This is close enough to EUR 66, based on the average value found in Germany and Italy for online shopping according to the OECD report, which is the most recent valuation of consumer detriment and consider to have a robust sample of consumers²⁸⁰ being surveyed but slightly further away than EUR 89, which is the average of the values considered in the fitness check (CIVIC, 2017). A **higher value of EUR 115** and based on the median values could be used as an upper bound (but this is the post-redress consumer detriment).

In estimating consumer detriment and in scaling up benchmarks for the estimated level of individual detriment, the following assumptions were made:

- There are 440 million consumers in the EU. 71% of consumers across Europe buying

²⁷⁴ CIVIC (2017): Study on measuring consumer detriment in the European Union. Main report, for DG Just.

²⁷⁵ Ipsos (2020): Survey On Scams And Fraud Experienced By Consumers, available at: [survey on scams and fraud experienced by consumers - final report.pdf \(europa.eu\)](#) and also at [factsheet fraud survey.final .pdf \(europa.eu\)](#)

²⁷⁶ Ipsos Ireland (2014): Consumer Detriment Survey Report.

²⁷⁷ The formula used to calculate the consumer detriment is as follows: Consumer detriment (EUR) = number of consumers experiencing a problem when buying on-line x (financial detriment from problematic experience + non-financial detriment from problematic experience). Refer to the methodological annex for more detail.

²⁷⁸ Note that the weighted average is 27.5% but we have rounded the figure to account for the consumers organizations responding.

²⁷⁹ Workbook: Consumer Market Monitoring Survey (tableau.com)

²⁸⁰ The target for each country was 1 000 online consumers, i.e. Internet users that have made at least one online purchase and who had encountered at least one e-commerce problem in the last 12 months. (OECD, 2022)

online.²⁸¹

- Approximately 30% of consumers experience some type of consumer detriment per year based on the findings from the consumer survey.
- It is estimated that 94m of consumers experience consumer detriment per year and either incurred a financial or a non-financial loss.
- The total consumer detriment has been estimated at between EUR 6.1bn and EUR 10.7 bn (using the median consumer detriment cost estimates per detriment).

For comparison, the earlier study **on consumer detriment supporting the 2017 Fitness check estimated that consumers suffered post-redress financial detriment of EUR 33.3 billion** (all type of channels and within six markets). This estimate however is considered as too high for this fitness check and may not reflect recent progress with the implementation of the MD and/or, more generally, efforts in implementation by competent authorities.

The impact assessment accompanying the proposal for a Directive on certain aspects concerning contracts for the supply of digital content showed the lack of clear contractual framework for digital content caused detriment to consumer. This detriment was estimated between **EUR 9-11 billion** in the EU just for music, anti-virus, games, and cloud storage service just for music, anti-virus, games and cloud storage services²⁸². **This estimate is more in line with the detriment estimated here.**

Thus, although consumer detriment is smaller in this fitness check (as it only covers the digital environment too), **this still carries a significant cost.** Consumer detriment includes both consumers experiencing a financial loss but also a higher percentage of consumers experiencing non-financial losses due to their time being wasted, stress, anxiety and frustration. It should be noted that the value used includes the financial loss due to time addressing the problem but excludes other type of non-financial detriment. This consumer detriment is likely to underestimate the total costs to consumers (financial and non-financial).

Furthermore, it can be observed that detriment may vary significantly depending on variations between different digital markets and sectors; but for practical reasons, the focus has been on estimating average detriment across digital products and services. It is important to consider that physical goods still represent a more significant problem for consumers than digital contents and services. There is a higher degree of sensitivity in the estimates of consumer detriment to any changes in the assumptions (either changes in detriment value or changes in the number of consumers affected). There are also attribution challenges in that whilst some consumer detriment is due to legal gaps and particular problematic practices not being covered in EU consumer law, in other areas, practices may already be prohibited, and detriment arises due to low to medium compliance by traders.

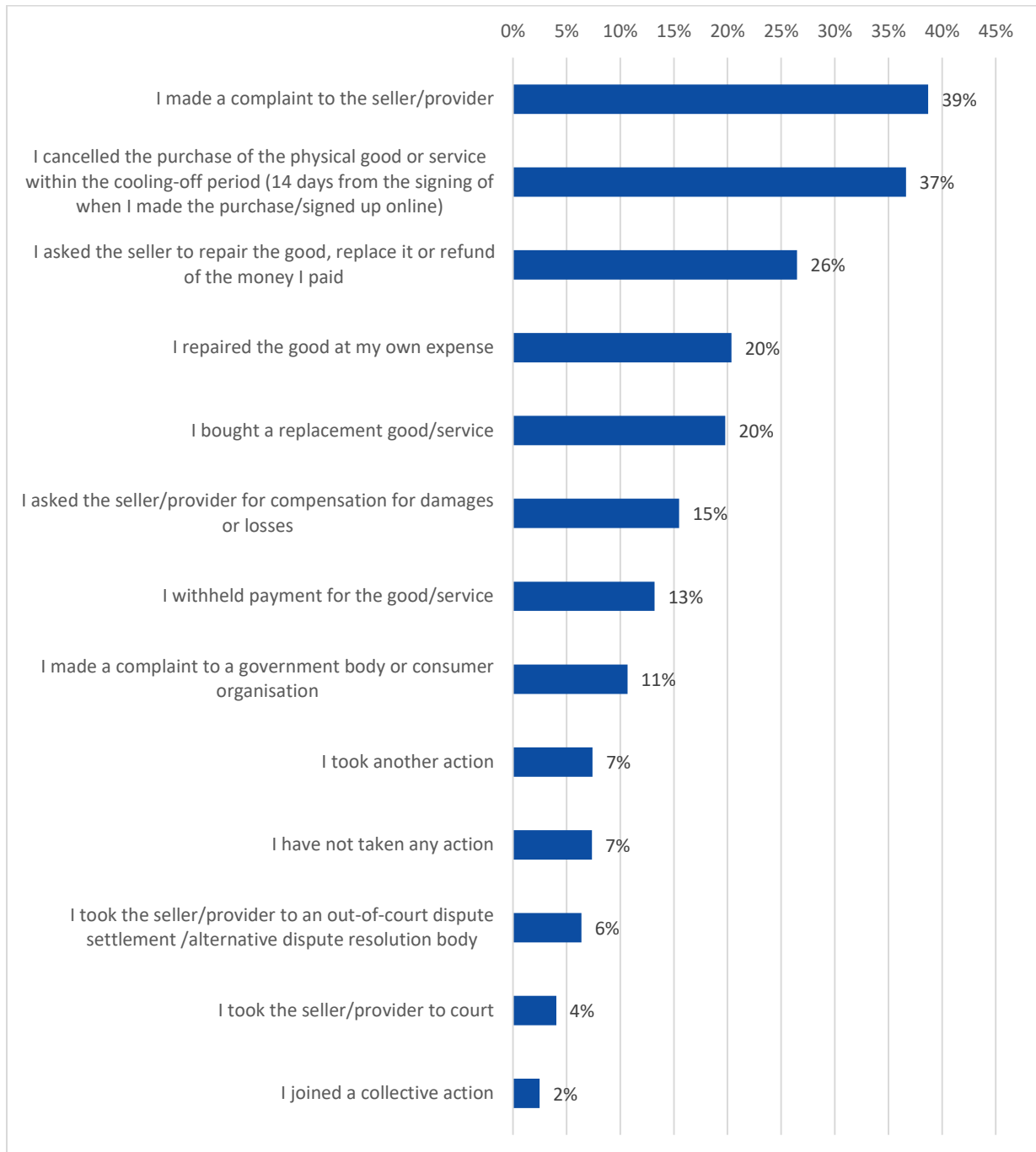
There are a few drivers affecting consumer detriment. These include lack of compliance by traders, low consumer awareness and/or lack of consumer action to follow up on the problem.

Indeed, the consumer survey revealed that **only 39% of consumers experiencing a problem made a complaint and 26% asked the seller to replace, repair or refund the money.** Moreover, 20% of consumers decided to repair their good at their own expense or bought a replacement, and only 15% asked for compensation for damages or losses.

²⁸¹ [E-commerce statistics for individuals - Statistics Explained \(europa.eu\)](#)

²⁸² ICF International, 'Economic Study on Consumer Digital Content Products', 2015

Figure 3.21 – Which of these, if any, have you done to sort out the problem? (n = 1537)

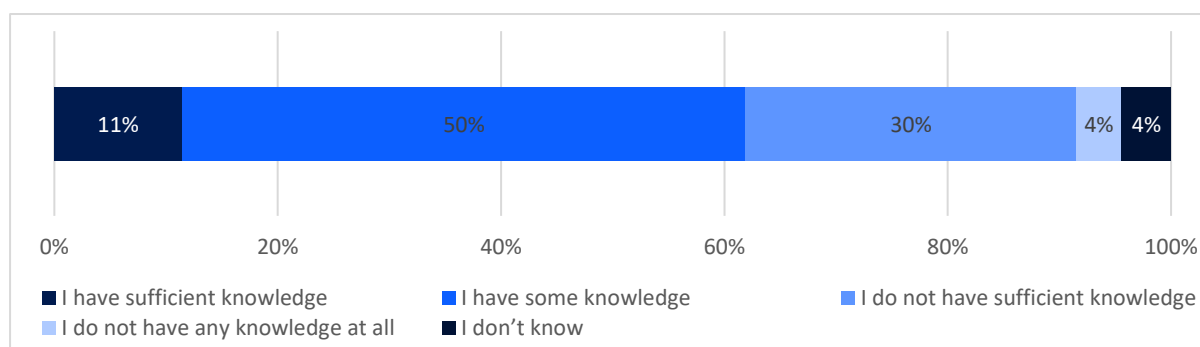


Source: consumer survey

The lack of action could also be due to lack of awareness by consumers about their rights. Only 11% of respondents to our survey noted that they have sufficient knowledge about consumer rights in the digital environment (see next figure). Our study has also found that there is a general lack of consumer awareness regarding the use of unfair practices. However, the study also found that once an unfair practice has been identified, consumers perceive these practices negatively.

The 2017 Fitness Check also concluded that there was a lack of awareness by consumers, and that this is an important impediment to a well-functioning consumer protection.

Figure 3.22 – 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)



Source: consumer survey

Increasing awareness will help consumers to exercise their rights and potentially reduce consumer detriment.

Levels of consumer detriment remain relatively high, as perceived by consumers in some of the surveys (e.g. public consultation, consumer survey). **Lack of compliance by traders** is an important explanatory factor regarding the ongoing high levels of detriment experienced by consumers.

Whilst there is no systematic data collected on levels of compliance by traders with EU consumer law requirements in the digital environment (or offline), some data was collected through primary and secondary data, such as through the public consultation and consumer survey as well as through sweeps carried out to check compliance by the CPC Network. For instance:

- 25% of respondents to the public consultation perceived that traders do not comply effectively with EU consumer laws in the digital environment.²⁸³
- Approximately half of consumers (46%) responding to the consumer survey noted that they had encountered problems relating to exercising the right of withdrawal²⁸⁴ (such as communicating with the seller, overly-complex procedures, and the lack of a clear means of exercising the RoW on digital interfaces).
- CPC Sweep on dark patterns (2022). National authorities from 23 Member States, Norway and Iceland checked 399 of websites and applications of retail sellers active in the sales of products for their own account. 42 websites used fake countdown timers with deadlines to purchase specific products; 54 websites directed consumers towards certain choices - from subscriptions to more expensive products or delivery options -, either through their visual design or choice of language; 70 websites were hiding

²⁸³ N = 350

²⁸⁴ N = 2745

important information or making it less visible for consumers. The sweep also included the apps of 102 of the websites screened, 27 of which also deployed at least one of three dark patterns categories.

- **CPC Sweep on Black Friday sales (2022):** 13 national authorities in the EU and EEA countries monitored the prices of 16.000 products from 176 websites with the aim of verifying how discounts are presented online. Overall, about 50% of the products monitored displayed a price reduction announcement on Black Friday. Among those, the authorities found that approximately one announcement out of four was inconsistent with EU law and that violations occurred in at least 43% of the screened websites.
- **Subscriptions sweep for this study:** Pre-contractual information about **cancellation procedures** for subscriptions is provided in 69% of cases, but this is less clear (or not mentioned at all) in 31% of cases. The clarity of information on **cancellation policies** was found to be mixed. The information was either clearly or very clearly presented (34.7% of cases), but a similar percentage for 'not clearly' and 'not at all clearly'.
- **Video games sweep for this study:** In 26.3% of games, the prices are only presented in the in-game currency and not in the real-world currency, making it confusing and misleading for consumers.

Further sweeps were conducted for this study (see Annex 4). The above demonstrate that across a range of primary and secondary data sources, compliance levels by traders vary and are not high enough to prevent significant levels of consumer detriment persisting.

Overall, consumers are likely to have benefited from more harmonised rules through EU consumer law and from pre-contractual information under the CRD and from more recent additional information disclosure rules under the MD to make informed decisions. As discussed in Section 2.2 on problematic practices by traders and in EQ4 focusing on enforcement, strengthening compliance and/or improving enforcement should have reduced levels of consumer detriment in theory over time e.g. as traders become more familiar with the requirements, as strategic deterrent cases taken on by CPAs have an incremental impact on traders' behaviours and practices over time etc.

However, in practice, levels of compliance by traders remain low, or at least, perceived problematic practices remain high. As shown in the effectiveness section on problematic practices, the public consultation and consumer survey found continuing high frequency with which consumers experienced such practices, commonly between one and three times annually across different areas. About one in three mentioned that they experienced detriment (either financial or non-financial harm) due to the problem encountered. The charts were provided in the effectiveness section and are also included in the stakeholder consultation section. In summary:

In the **public consultation:**

- 89% experienced dark patterns in website or app design;
- 75% reported a lack of disclosure regarding paid promotions by social media influencers;

- 74% thought personal data was misused or used unfairly to personalise commercial offers;
- 62% perceived a contract term to be unfair when buying a digital service or digital content, but nevertheless had to agree to it; and
- 53% had difficulties cancelling digital subscriptions.

74.4%

The number of consumers who stated personal data was misused (or used unfairly) to personalise commercial offers at least once per year (public consultation).

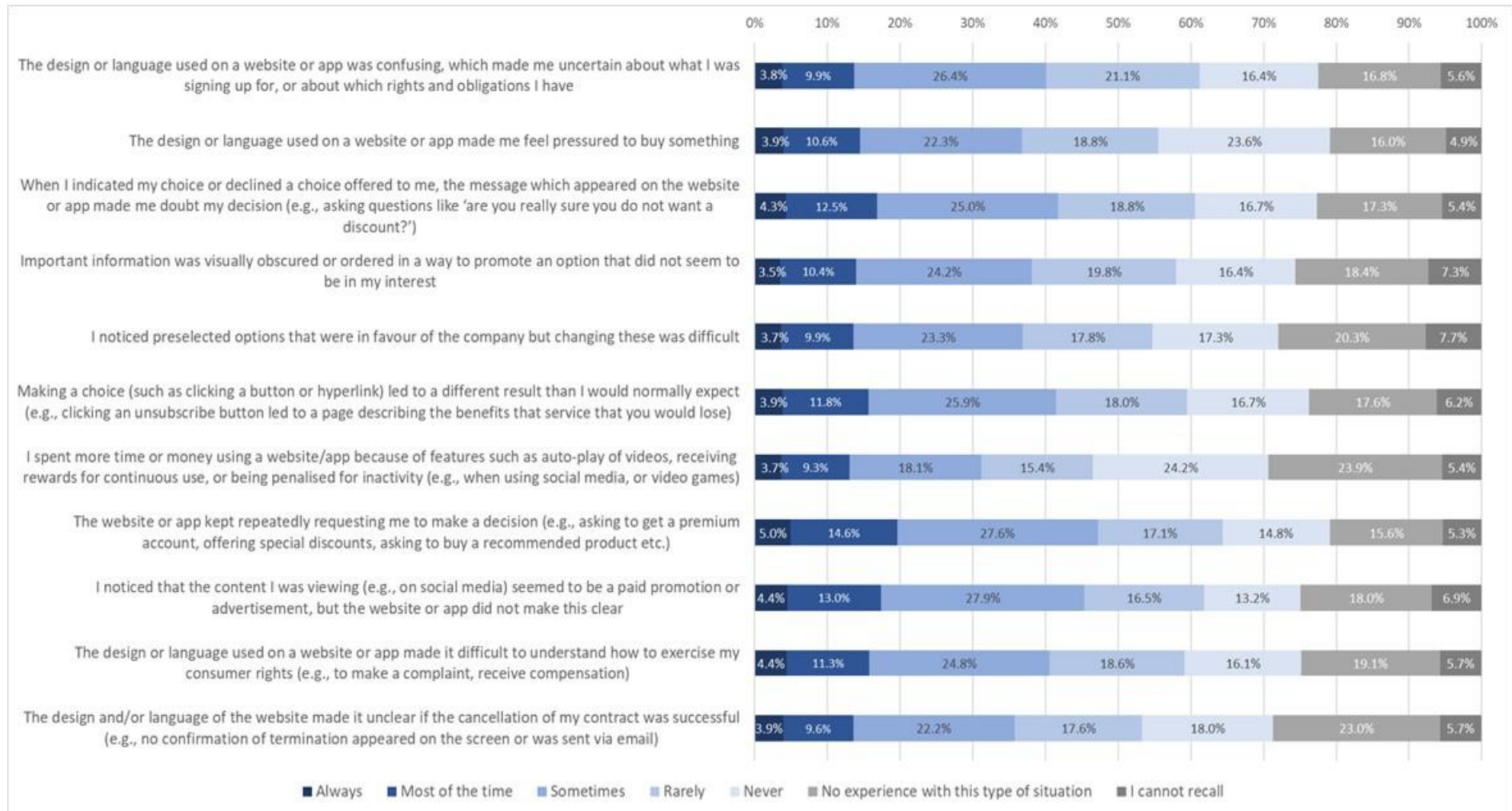


In the **consumer survey**:

- 32% paid more than they planned to because during the purchasing process the final price changed to a price higher than the one advertised initially;
- 48% experienced repeated requests/nagging for the consumer to make a decision, e.g. to get a premium account, offering special discounts, asking to buy a recommended product; and
- 37% had impression that companies had knowledge about their vulnerabilities and used this for commercial purposes (most prominent among 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').

The full results from the consumer survey question on the incidence of problems encountered (which will lead to detriment for a proportion of consumers affected) are shown in the following Figure. In essence, these show that high levels of problematic practices remain from a consumer perspective, and in a further question about detriment, about 30% experienced financial or non-financial harm resulting from the problems experienced:

Figure 3.23 – Consumer survey: In the past 12 months, have you experienced any of the following situations online, and how frequently? (n = 10,000)



3.2.4.2 Scale of problem of problematic practices and associated consumer detriment

The purpose of this sub-section is to consider the scale of the problematic practices examined in detail in Section 2 and to assess consumer detriment in the digital environment for specific problematic practice areas, quantitatively where possible, but mainly qualitatively.

Methodology for assessing consumer detriment in the digital environment at the level of problematic practices

Types of consumer detriment: examples of detriment include **personal, structural and hidden detriment**. A typology of different types of harm caused by detriment to consumers in a digital context was presented earlier. This includes **financial harms**, such as financial loss due to an ongoing subscription the consumer wanted to cancel through to it being difficult to cancel an online subscription due to dark patterns or the lack of a reminder and **non-financial harms**, such as the consumer's time being wasted unnecessarily.

Aims: this thematic assessment seeks to quantify the problem's scale and where possible, to assess the degree of consumer detriment among problematic practices identified in the digital environment within the EU's (digital) single market. The study aimed to compare the scale of the problem and extent of consumer detriment being experienced by European consumers in the 2016-17 period as a baseline in comparison with today.

Methodology for assessing the scale of problem across different problematic practice areas and the level of detriment in the 2016-17 period compared to 2023-24.

The **scale of the problem** has been estimated using (1) survey data on the incidence of problems encountered in the digital environment by consumers and (2) perceived detriment levels among consumers regarding these problems. This has then been contrasted by the change in market size and structure during the intervening period, as it is important to contextualise the problem's scale as 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 in absolute value terms, even if the problem has remained constant (though in such an illustration the proportion of detriment to market value would have remained the same. However, the magnitude of the problem would need to be assessed in more detail through a future possible impact assessment.

Regarding the **assessment of consumer detriment across different types of digital problematic practices with an impact on digital fairness**, the frequency of detriment was first considered using survey data for the present situation and secondary data (usually survey-based, but sometimes based on modelling projections) for the baseline assessment to analyse the evolution in detriment levels. A distinction was made where possible between different types of harms, such as financial and non-financial harms, for instance when reviewing secondary literature, but estimates were often limited and/ or not disaggregated by type of harm (see methodological challenges below).

The previous fitness check in 2016-17 adopted a similar approach when making estimates as to the extent of detriment based on survey data among consumers regarding the frequency of problems experienced and the associated level of detriment. To complement the survey-based quantification of overall detriment across digital markets and services, desk research was undertaken to identify and review relevant secondary literature addressing consumer detriment across specific thematic problematic practices in the digital environment, such as subscription traps and loot boxes. 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 2016-17 period, with a view to analysing problematic practices and determining how far these evolved between the baseline and current situation.

Previous studies provided some **useful benchmark data** in relation to **estimated average detriment per consumer** in areas such as subscription traps and within the dark patterns topic, in areas such as drip pricing. However, the few benchmarks that were obtained come from different time periods, **making it difficult to establish a uniform, time-specific baseline for all problematic practices**. However, this is inevitable given that some practices did not exist, or were only very emerging back in 2016-17.

Methodological challenges and data limitations: key challenges in establishing a baseline regarding the problem's scale were:

- The wide-ranging study scope as many problematic practices in the digital environment were covered;
- Differences in focus between the previous fitness check in 2017-17 did not focus on digital fairness, although one or two problematic practices, such as subscriptions, were referenced in both studies;
- The fact that some problematic practices are relatively new and whilst studies have been undertaken on them recently in the 2020-2024 period, there is a lack of literature on the extent of the problem dating back to the 2016-17 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 be exercised in directly comparing different study's survey results given different survey cohorts, differences in question phrasing, etc.).

The scale of the problem was nonetheless estimated by using secondary literature and comparing with the current study's survey findings, as the public consultation, consumer survey and the targeted survey asked relevant questions about business practices in the digital environment considered problematic by at least some, and sometimes the majority of consumers (see effectiveness section for detailed examples).

Turning to methodological challenges in assessing detriment, these were that:

The previous fitness check (FC) estimated detriment but the study covered offline and online sectors so is not directly comparable. There is also only limited alignment with the current study, as the latter focuses on a wider range of problematic practices in the digital environment, reflecting key differences in study scope. The legal scope was also different between the two studies, as the 2016-17 FC covered marketing law not only consumer law.

Whilst it was possible to **partially reconstruct a baseline** retrospectively, there was no single dataset that could be used as a starting point. Whilst some relevant earlier studies and survey-based data were identified to reconstruct the baseline, caution should be made when comparing the results as different studies asked survey respondents questions that may have differed in wording from the present fitness check.

Nonetheless, the research identified examples of earlier thematic studies that focused on problematic practices such as subscription traps, which provide **insights into whether the situation has remained the same, got worse or better over time**. Whereas survey-based data on consumer perceptions as to the scale of the problem were identified for most business practices identified as potentially problematic, but only a few of these studies estimated detriment.

Assessing consumer detriment is itself methodologically complex, although as noted in the efficiency section, improvements have been made in methodologies to quantify detriment, for instance, through the 2017 Study on measuring consumer detriment in the European Union (EU) Study.²⁸⁵ The OECD subsequently did work on improving measurement of consumer

²⁸⁵ European Commission, Consumers, Health, Agriculture and Food Executive Agency, *Study on measuring consumer detriment in the European Union – Final report, Part 1 – Main report*, Publications Office, 2017, <https://data.europa.eu/doi/10.2818/87261>

detriment in 2020. This demonstrates that approaches to assessing consumer detriment more effectively have only evolved in the intervening period and therefore, earlier research to inform the baseline often lacks estimates of detriment. The difficulties in quantifying detriment in areas receiving increased regulatory attention at EU level and internationally such as dark patterns has been recognised by the OECD. For instance, the OECD noted in a 2022 research paper on dark patterns that *“Dark commercial patterns are business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances”*.²⁸⁶

When considering the problem’s scale, it is worth stressing that digital problematic practices considered through this study are themselves **heterogeneous, and have emerged as perceived problems among consumers at different points in time**. Moreover, whereas some problematic practices are longstanding, such as subscription traps, others have emerged more recently, and there is either no baseline data (or only limited) available from 2016-17. For instance, whereas video games were already prevalent by that time, some specific problematic practices, such as the lack of transparency in payments for virtual items/ use of virtual currencies within games and problems around loot boxes (digital addiction, high cost of loot boxes for children and widely increased accessibility of such games to minors due to ubiquity in availability of smart phones and tablets, absence of transparency on randomisation odds) have emerged more recently.


Therefore, the baseline has had to be staggered in a way that reflects the fact that digital markets and services are fast-developing and innovative sectors, with some problems only emerging more recently. Therefore, monitoring should be undertaken in future to follow-up on the present study. For instance, surveys to assess the longitudinal evolution of digital fairness could be undertaken once every three or five years to assess the evolution in the scale of the problem over time. This would enable EU and national policymakers to keep track of how far existing consumer rules, guidance and enforcement are having a positive effect in tackling the problem (or not).

1. The scale of the problem by problematic practice

A summary of the problem’s scale by problematic practice is provided below. This seeks to establish a baseline to the extent possible and compare the situation with the 2023-24 period during which the study was conducted. In the follow-up supporting table, more detailed information regarding the sources for the benchmarks taken from previous studies and surveys is provided. The extent to which estimates of detriment were also available by problematic practice is also provided.

²⁸⁶ OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm>

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

<p>or uncontrolled spending.</p>	<p>and paid apps, including loot boxes.²⁸⁹</p>	<p>68% of respondents agreed that loot boxes and addiction-inducing design features were the problematic practice which were perceived to have increased the most in frequency in the last five years. 75.7% of respondents agreed that the usage of loot boxes and addiction-inducing design features (in digital services such as video games are problematic. Consumer survey: 16% of consumers who had used or purchased digital content/services/subscriptions in the past 12 months indicated experiencing challenges when making in-app purchases because prices were displayed in the app's virtual currency.</p>	<p>features such as in-app currencies and loot boxes increased.</p>	
<p>Personalisation practices, incl. behavioural advertising and personalised pricing</p> <p>Data misuse for personalised commercial offers, use of sensitive data. Absence of transparency if traders are non-compliance regarding disclosure requirements, lack of information as to whether personalised prices benefit or</p>	<ul style="list-style-type: none"> In 2018, 49% consumers were concerned about how their personal data is used and shared (Commission study on online market segmentation through personalised pricing/offers). In 2018, between 12% to 20% of consumers had bad experiences related to personalised pricing.²⁹⁰ 61% of 160 e-commerce websites studied practiced 	<p>Consumer Conditions Scoreboard 2023: 70% of consumers are concerned about how their personal data is used and shared (21 percentage point increase compared to 2018). Public consultation: Three-quarters of respondents to the public consultation said that within the last 12 months they had experienced situations where their personal data was misused or used unfairly to personalise commercial offers (45.1% said this occurred 3 or more times, and 29.3% once or twice). Consumer survey: 74.3% of respondents reported that they were victims of data misuse for personalised commercial offers. 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.</p>	<p> <i>c. 21pp increase in problems with the use and sharing of data in the B2C context</i></p>	<p>To complement the GDPR, the Modernisation Directive, DSA and DMA strengthened the transparency and fairness of personalisation practices, especially for online platforms. However, problems have increased, given the general growth in personalised ad markets, and a lack of clarity on the boundaries of acceptable personalisation in commercial practices and what amounts to an unfair use of data. Baseline data is often lacking on these issues given they have more recently post-GDPR in 2018 become more prominent in policy discourse, studies and research. Modernisation Directive has strengthened transparency of personalised pricing and the ranking of search results on platforms. There remains a problem that consumers may be informed about a price being personalised but they have no idea whether this benefits or disadvantages them. Furthermore, price personalisation based on the willingness to pay may be perceived as unfair.</p>

²⁸⁹ Loot boxes in online games and their effect on consumers, in particular young consumers - [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU\(2020\)652727_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU(2020)652727_EN.pdf)


²⁹⁰ Consumer market study on online market segmentation through personalised pricing/offers in the European Union - https://commission.europa.eu/system/files/2018-07/exec_summary_online_personalisation_study_en.pdf

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

<p>disadvantage consumers.</p>	<p>“personalized ranking of offers.</p> <ul style="list-style-type: none"> • Across the EU, more than two-thirds (71%) of respondents in the consumer survey reported that in their experience nearly all or most websites use online targeted advertising. 54% stakeholders reported that targeted adverts in their various forms are in their opinion used by “most websites” or “nearly all websites”.²⁹¹ • Overall, the share of websites practising personalised ranking of offers was 92% for the airline ticket websites, 76% for hotel room websites, 41% for the websites selling sports shoes, and 36% for the websites selling TVs. Almost three in ten respondents (28%) in the consumer survey reported that they believed nearly all or most websites use online personalised pricing. 	<p>37% of consumers had the impression that the company had knowledge about their vulnerabilities and used it for commercial purposes.</p> <p>34% of consumers did not have the option to opt-out of personalised commercial offers (e.g. personalised prices or advertisements).</p> <p>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.</p> <p>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</p> <p>Targeted survey - 53.1% of consumers perceived that personalised pricing has increased in frequency.²⁹²</p>		
--------------------------------	---	--	--	--

²⁹¹ European Commission (DG JUST) - Consumer market study on online market segmentation through personalised pricing/offers in the European Union (2017). https://commission.europa.eu/system/files/2018-07/exec_summary_online_personalisation_study_en.pdf

²⁹² Targeted survey: (Qs. In the past five years, how far have the following potentially problematic B2C digital practices increased or decreased in frequency? (N = 90)

<p>Dark patterns</p> <p>Unfair design interfaces, cancellation difficulties, increased cost of transactions due to drip pricing, etc.</p>	<ul style="list-style-type: none"> In 2018, CPAs across the EU screened 560 e-commerce sites offering various goods and services. On 211 of the 560 websites the final price at payment was 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.²⁹³ 	<p>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.</p> <p>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.</p> <p>Public consultation: 88.7% of respondents mentioned they found website or app designs confusing or deceptive (48.6% 3 times or more and 40.1% once or twice with only 9.5% never experiencing this issue)</p> <p>Targeted survey: 74% of respondents reported the presence of deceptive practices (dark patterns) in websites/app design.</p> <p>Consumer survey: 20% of consumers surveyed indicated that they have often experienced a website or an app repeatedly asking them to make a decision online.</p> <p>15% of consumers said that they have often experienced a situation with a virtual assistant device where they were charged for a purchase that they did not intend to make.</p>	<p style="text-align: center;"></p> <p>Qualitative judgement as no directly comparable baseline data.</p>	<p>Whilst direct comparative information is not available, there has been a proliferation of research and policy/enforcement interest in dark patterns in the last few years.</p> <p>There have been reports of various misleading online practices (e.g. drip pricing, subscriptions traps, hidden information), but these were not previously labelled as 'dark patterns' but simply as consumer law breaches.</p>
--	---	---	--	---

²⁹³ https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/previous-sweeps_en

3.2.4.3 Benefits for consumers

EQ6(3) – Are there any benefits of practices identified in the digital environment that may partially offset consumer detriment?

Whilst there are costs for consumers due to different types of detriment associated with the problematic practices under review, the general benefits for consumers in the digital environment, including in relation to some of the practices identified as problematic, should not be overlooked. General benefits for digital consumers include: easy access to, and wider choice of goods and services in the online than in the offline environment, greater ability to interact with traders and to comment on their experiences of using goods and services and personalisation.

However, sometimes there are both positive benefits and negative impacts of particular business practices. For instance, taking a topic such as personalised advertising, some detriment was identified for instance if data is mis-used, sensitive data is used without consumers' consent and/ or if behavioural research to test consumers' emotions and purchasing patterns is used based on gathering their personal data. However, there are equally benefits of personalised advertising, such that a high percentage of consumers are willing to provide their personal data even if a certain percentage have concerns about such advertising and/ or may wish to opt out altogether of such ads. Wider EU legislation beyond consumer law affords some degree of protection.

There are trade-offs between consumer detriment experienced by a proportion of consumers due to personalised ads being seen as intrusive, whereas other consumers (some studies pointing upwards of 80%) may view personalisation as being helpful with consumer benefits as content and/ or ads are made more relevant to them using the consumers' personal data. Therefore, assessing costs and benefits is complicated by the fact that many consumers experience general benefits in the digital environment even though some experience detriment. However, this does not suggest there is no problem, rather that the problem is multi-faceted as some business practices may have elements that are beneficial for consumers, providing them with the types of products and services they want and need, but also elements that are unfair.

The same is true of online subscriptions. The subscription economy has tripled in size since the baseline in only 7 years (see market assessment in Section 3.2.2). Therefore, consumers must see there being inherent benefit in subscriptions otherwise they would not have significantly increased take-up of subscriptions. However, the existence of these benefits does not mean that there are no disbenefits or detriment, for example due to difficulties in cancelling online subscriptions when no longer needed.

In conclusion, consumers may also benefit from at least some of the practices examined where some problematic practices were identified.

EQ6(4) – What are the main benefits of consumer law Directives in theory? How far have these actually been manifested in practice?

Having a regulatory framework that is fit for purpose can increase consumers' confidence to conduct digital transactions. Eurostat mentions that 68 % of individuals in the EU ordered or bought goods or services over the internet for private use in 2022. The latest Consumer Conditions Scoreboard (CCS) 2023, showing data gathered in 2022, shows that the **percentage of consumers conducting online transactions has increased from 57.8% in 2016 to 71% in 2022** (+23.2pp), suggesting increased take-up among consumers in

conducting transactions and signing up to services in the digital environment.

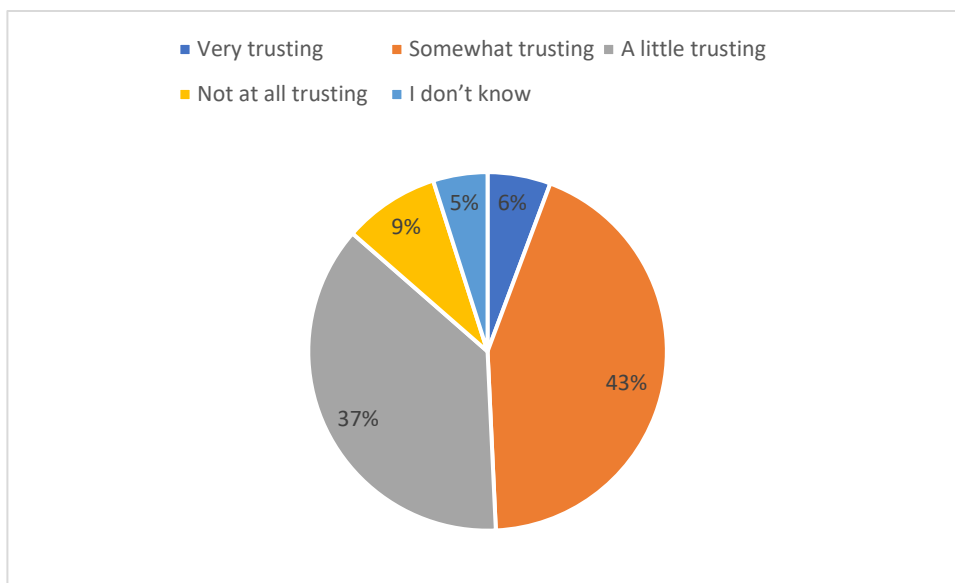
The increase in online shopping is also partly driven by wider digitalisation of the European economy and society and cannot solely be attributed to more effective application and enforcement of EU consumer law, which has played a role, but is one among several factors leading to increased online purchases (digitalisation, catching-up in performance of MS where previously there was a reluctance to engage in online shopping²⁹⁴).

In the CCS 2023, 76% of consumers agreed that retailers and service providers respect consumer rights, without distinguishing between the online and offline environment. However, *“trust levels vary by different demographic characteristics, e.g. by age, level of education and financial situation. 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”*.

For **EU citizens/ individual consumers**, there is more uniform level of protection in the digital single market and arguably lower prices than would otherwise be the case were there to be 27 different pieces of national consumer legislation in the areas covered by the three Directives (e.g. unfair practices and contract terms). **Consumer associations** were strongly positive about the benefits of EU consumer law overall. However, key EU associations such as BEUC expressed concerns regarding the potential benefits being undermined due to the problem of digital asymmetry that consumers face (reference should be made here to Section 3.2.2 which considers this issue in more detail and to EQs under effectiveness). There were also concerns that enforcement is insufficiently strong and harmonised (e.g. levels of resourcing among CPAs) across the EU-27 that problems such as dark patterns in website and interface design remain and other challenges such as hidden advertising are insufficiently policed (e.g. influencer marketing). This was seen as undermining potential benefits such as reducing consumer detriment.

The percentage of consumers that engage in digital transactions has increased considerably in the past decade, which could be used as a proxy for increased consumer trust in completing transactions relating to products and services in the digital environment. The consumer survey asked about trust among consumers in online business and websites. The following figure sets out the responses.

Figure 3.24 – How trusting are you of online businesses and websites? (n = 10,000)



²⁹⁴ Eurocommerce report on e-Commerce in Europe showed significant differences in levels of willingness to make e-commerce purchases between consumers in different MS, reflecting differing levels of consumer trust, and also cultural factors.

Source consumer survey

Almost half (49%) of respondents were either very trusting or somewhat trusting. Less positively, 46% of consumers combined either have limited trust in online traders (37% are only a little trusting), or do not trust online businesses and websites at all (9%). These findings suggest reflect a paradox that despite increasing levels of consumers conducting transactions in the digital environment, persistent problematic practices remain, meaning that even if consumers are increasingly are digitally active given ongoing digital transformation of the society and the economy, due to the ongoing persistence of problematic practices, a significant proportion do not have strong trust in traders when conducting transactions.

A study on the impact of consumer protection in the digital age, based on evidence from 2006 to 2014 in the EU, found a significant relationship between the introduction of the UCPD and consumer trust and cross-border purchases for countries with a low consumer protection level before the introduction of the UCPD. The relationship was found to increase over time and stay then relatively constant.²⁹⁵ It is certain that consumers benefit from increased protection in the digital market which increases their trust (this finding was also shared by the earlier evaluation of the CRD; CEC, 2017). Additionally, consumer benefit from reduced prices online.

There are studies quantifying the increase in consumer welfare from digital shopping or free online services²⁹⁶ but the consumer welfare benefits from the application of EU Consumer law (through the UCPD, the UCTD and the CRD) in e-commerce have not previously been monetised in relation to the digital environment. Therefore, previous studies of analogous relevance have been analysed. For instance, the impact assessment of Directive (EU) 2019/771 on the Sales of Goods noted that consumers could benefit from a decrease in consumer prices of 0.25% resulting from fully harmonised rules in e-commerce.

The findings from this study are replicated below and show an increase in consumer welfare of EUR 18bn²⁹⁷, which may underestimate the total benefits as the digital activity was lower than it is currently.²⁹⁸

Increase in consumer welfare due to harmonised rules in e-commerce

Consumers would enjoy better prices and an increased variety of offers. Just looking at e-commerce, fully harmonised rules would **increase consumer welfare**.

Increased competition will lead to increased availability of a wide variety of products at more competitive prices. Consumer prices would drop in all Member States, ranging from -0.35 % in Spain to -0.05 % in Lithuania and Romania. The average decrease in consumer prices across the EU can be estimated at -0.25 %. Household consumption, which mirrors consumers' welfare, would equally rise in every Member State, ranging from +0,05 in Lithuania to +0.38 in Spain, with an average of +0.23 for the EU28. **This corresponds to about EUR 18 bn** (but assumed a much lower percentage of digital activity, 15%, so may be underestimate the total benefits due to the increase in e-commerce).

If consumers were to shop more cross-border online or offline, they could take advantage of existing price divergences between Member States. For example, a Swedish consumer could pay 32 % less buying clothes in Germany while a Maltese consumer could pay 23 % less buying household appliances in Italy. Whilst these price differences do not take account of factors such as differences in taxation and delivery costs (in part to be addressed by other initiatives in the Digital Single Market strategy), they nevertheless point to important potential opportunities for consumers.

²⁹⁵ Anja Rösner, Justus Haucap, Ulrich Heimeshoff (2020): The impact of consumer protection in the digital age: Evidence from the European Union, International Journal of Industrial Organization, Volume 73,2020,

²⁹⁶ See discussion in [Consumer Welfare in the Digital Economy – Report on the Digital Economy \(gaidigitalreport.com\)](https://gaidigitalreport.com)

²⁹⁷ SWD (2017): the Impacts of fully harmonized rules on contracts for the sales of good supplementing the impact assessment accompanying the proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods. SWD/2017/0354 final: [EUR-Lex - 52017SC0354 - EN - EUR-Lex \(europa.eu\)](https://eur-lex.europa.eu/lexuri/cs/l/fr/?uri=CELEX:52017SC0354-EN)

²⁹⁸ The consumer welfare gains from an integrated EU market for e-commerce in goods assume a 15 % share of internet retailing.

Finally, consumers would benefit from a wider variety of offers: it has been estimated that **lower online prices would constitute just one third of the total consumer welfare gains** from an integrated EU market for e-commerce in goods, as two thirds of the gains would come from increased choice.

Therefore, a single set of EU-wide high consumer protection rules would further empower EU consumers to take advantage of an increased offer and strengthened market competition, thus directly contributing to the shaping of a true single market.

Source: SWD(2017) 354 final²⁹⁹

Benefits to consumers from disclosure of information resulting from the MD will also be relevant. The Impact Assessment to the MD concluded that more transparency on online marketplaces would increase consumer protection and in their public consultation, all consumer associations and public authorities, as well as almost all citizens agreed that this would bring benefits for the consumers (2018³⁰⁰).

54% of respondents to the public consultation to this fitness check³⁰¹ concluded that the existing EU consumer law framework has had **a very positive impact or a rather positive impacts on the amount and relevance of information available to consumers to compare and make informed purchasing choices; and 27% thought that this has benefited them in terms of product pricing.**

3.2.5 Costs and benefits for consumer protection authorities

EQ6(3) – What are the regulatory compliance costs (administrative, adjustment costs) and benefits of the Directives for CPAs?

Costs and benefits for CPAs of ensuring compliance with EU consumer law in the digital environment

- CPAs responsible for monitoring and enforcing EU consumer law face additional costs when carrying out their responsibilities in the digital environment. This is due to various factors, such as the complexity of undertaking surveillance and enforcement in the digital environment.
- Examples of additional costs related to the implementation of the consumer law directives in the digital environment include: checking websites for deceptive designs, applying the fairness test in a digital context e.g. investigating whether websites or platforms' use of algorithms may be unfair, misleading, or aggressive.
- Given the opaqueness of the technologies concerned, and the need to make information requests to traders for further details, there is considerable complexity in assessing whether traders are fully compliant, and whether an enforcement action can be justified and stands a good chance of success and/ or serving as a strategic deterrent.
- Further costs for CPAs in implementing consumer laws in the digital environment were found to have arisen due to the increased complexity of enforcement actions, either because of the technologies and digital interfaces involved compared with offline enforcement or because of the challenge that multiple different laws may be applicable in parallel when investigating traders. For instance, some enforcement activities solely fall within consumer law, such as problematic practices already covered by the UCPD, others involve growing complexity due to the increased interconnectedness between the applicability of EU consumer law in parallel

²⁹⁹ Commission Staff Working Document on the Impacts of fully harmonised rules on contracts for the sales of goods supplementing the impact assessment accompanying the proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, available at eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0354

³⁰⁰ Page 65. [resource.html \(europa.eu\)](http://resource.html.europa.eu)

³⁰¹ n = 221 responses to this question

with data and digital laws.

- This in turn means some enforcement activities and legal cases undertaken by CPAs are highly complex, requiring specialist legal and technical expertise, which is costly both in human and financial resources.
- The main source of information on the incidence of costs came from the targeted survey. Evidence for the higher costs for CPAs of enforcement in the digital environment also came from the interviews and review of case law. It was noted that there are comparatively few pieces of case law driven by CPA-led enforcement cases. Interviewees from CPAs such as consumer ombudsmen noted that whilst individual cases can be more costly in the digital environment, this has driven CPAs to instead take on fewer cases overall, but to take on strategic deterrent cases with important implications for wider traders in the digital environment. This in turn should deter traders from non-compliance and/ or bad practices in future, thereby helping to reduce enforcement costs for CPAs.

Costs and benefits for CPAs of ensuring compliance with changes through the MD

- The changes made through the MD (some of which apply in the digital environment) did not appear to have resulted in that many additional costs for CPAs, at least only between 18% and 25% of CPAs perceived the costs across different areas to be significant, whereas 50% perceived there to be no costs at all.
- The most significant costs of applying the MD and consumer law in the digital environment generally were found to related to inspection, i.e. checking that traders are compliant.
- An explanation why CPAs perceived the costs of implementing the MD changes to be relatively modest were that some of the new requirements can be checked relatively easily e.g. whether information disclosures are prominent on platforms as it requires a simple check, checking whether a sample of online reviews on platforms are genuine.
- The benefits for CPAs of the MD's introduction are greater regulatory clarity regarding which practices are prohibited (e.g. scalper bots for event tickets, fake online reviews), which are regulated (e.g. information disclosures around automated personalised pricing and criteria used in search rankings).
- These changes were seen as reducing regulatory uncertainties and helping to promote improved compliance as some digital-specific rules have been introduced where previously the rules lacked detail.
- Whilst it is generally too early to assess the benefits of the MD for CPAs given there have as yet not been more than one or two enforcement cases across the EU-27, there could in future be a reduction in the costs for CPAs.
- Greater regulatory certainty and less reliance on the guidance could help to reduce the legal costs for CPAs of taking enforcement actions, including bringing legal cases against traders.

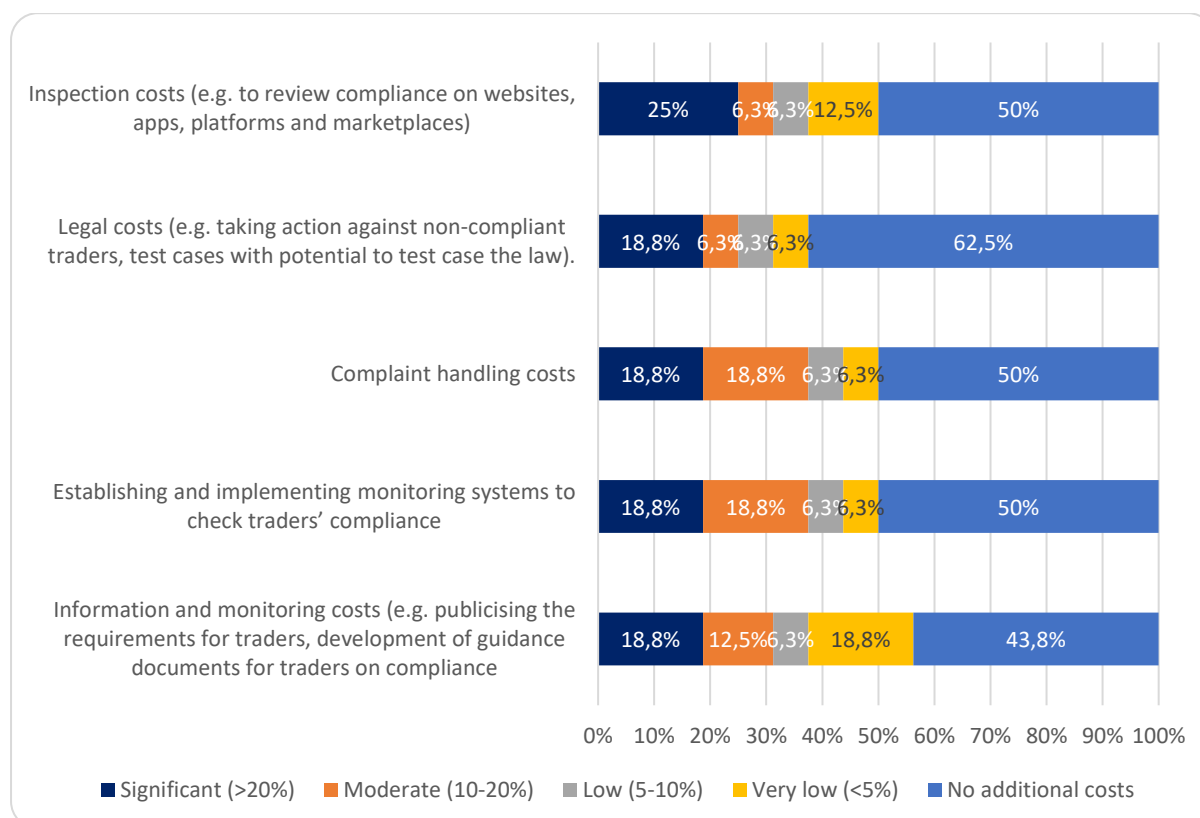
Table 3-10 – Overview of costs of compliance with (and enforcement of) EU consumer law by stakeholder type

Types of administrative costs	Types of adjustment costs
Enforcement and monitoring costs of traders' compliance with consumer law. Costs of proceedings/sanctions/injunctions. Costs of training. Following national case law and any CJEU rulings across the EU-27 to help interpret the	Training CPA staff in investigating compliance with EU consumer law in digital environment. Adapting investigation and non-compliance detection practices to meet requirements of digital age. Examples: using web crawlers and developing IT tools to check for compliance in websites/applications and contract terms.

Types of administrative costs	Types of adjustment costs
application of EU consumer law.	
Reading the guidance documents for the UCPD, UCTD and CRD.	

The targeted survey asked authorities about the different types of costs associated with the Directives and changes due to the MD³⁰². The following figures shows their responses. As it can be seen, the most significant costs are related to inspections. More moderate costs stem from complaint handling cost and establishing and implementing monitoring systems to check traders' compliance.

Figure 3.25 – To what extent have the regulatory amendments made to the three consumer law Directives due to the transposition and application of the Modernisation Directive led to any additional costs for your authority? Have the enforcement costs for your authority been significant, moderate or low? (N = 16)



Source: targeted survey

16 CPAs replied to this question out of a total of 20 enforcement authorities that responded to the targeted questionnaire. Whilst this is a small cohort of responses, it should be recalled that these respondents are national level CPAs, and the responses therefore ought to be reasonably representative.

Regarding the types of costs, the consultation findings show that following the MD, only circa one in five to one in four of CPAs saw the costs of carrying out enforcement activities as being

³⁰² Q55: To what extent have the regulatory amendments made to the 3 consumer law Directives as a result of the MD led to additional costs for your authority?

more costly following the MD, which includes some additional digital-specific compliance requirements:

- Inspection costs to check compliance on websites were viewed as incurring significant costs by 25% of respondents and moderate costs by 6.3%. Conversely, 50% said no additional costs and a further 12.6% said either low or very low costs.
- Regarding complaint handling costs and establishing monitoring systems to check traders' compliance, there were similar responses for both. 18.8% saw these costs as being significant and a further 18.8% moderate. In contrast, 50% saw no additional costs.
- Most CPAs (62.5%) did not identify additional legal costs from taking additional action against non-compliant traders. 18.8% saw these costs as being significant and a further 6.3% moderate.
- Lastly, regarding information and monitoring costs, such as publicising new requirements under the MD to traders, developing guidance, 18.8% saw these costs as being significant and a further 12.5% moderate. In contrast, 43.8% saw no additional costs, and a further 25.1% either low or very low costs (18.8% very low costs and 6.3% low costs).

In the interview programme, CPAs provided general feedback that there are increased costs of applying EU consumer law in the digital environment due to the complexity of the EU legal landscape, and the fact that often, enforcement cases are complex and can involve a combination of consumer law, digital and/ or data laws. There do not appear to be specific additional costs stemming from the digital-specific changes brought about by the MD. This may be because some of these are relatively straightforward for traders to implement and for CPAs to check traders' compliance, for instance with new information disclosures for marketplaces.

Additional costs instead relate to 1) applying consumer law in the digital environment stem due to the complexity of applying different laws in parallel and 2) the fact that some problematic practices are difficult and complex to investigate as there are grey areas, where there may be complaints about traders' business practices, but gathering sufficient evidence to go ahead with enforcement actions and especially taking on legal cases requires complex investigation.

CPAs interviewed mentioned that digital-related strategic deterrent cases were often found to relate to EU consumer law being applied in conjunction with other types of digital and data laws. The added complexity and requirement for a broad range of expertise in digital technologies and legislation to take on enforcement cases were considered as costly, compared with cases in the offline environment.

For example, investigating whether AI algorithms underlying which types of information consumers see and whether some consumers face restricted choices or investigating and proving dark patterns exist requires research into opaque technologies and design interfaces, which is time-consuming and technically-complex.

As for the benefits of the MD from a CPA perspective, these stem from increased certainty on the application of consumer law rules to the digital environment, given there are several new digital-specific requirements. There could be further benefits from a reduction in breaches due to deterrence in the form of fines under the MD or UCPD remedies. The impact assessment of the MD acknowledged that strong civil remedies and the possibility of escalating the complaint to national courts and enforcement authorities could incentivise traders to settle more complaints on a voluntary basis, thus reducing the costs for CPAs. Moreover, it could also benefit them as authorities in other MS also take effective enforcement against cross-border traders.

Lastly, it should be stressed that as the MD is relatively new, CPAs lack experience in applying the new provisions as integrated into national laws through the regulatory amendments to the underlying legislation (the UCPD, CRD and the UCTD). There was therefore limited feedback on the MD's application from an enforcement perspective, and therefore CPAs found it difficult to provide estimates of any changes in their costs.

3.2.6 Proportionality of costs and benefits

EQ6(4) – 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 the society?

The main costs for traders relate to familiarisation and checking compliance but these are mostly for cross-border trading. Such costs would be mitigated by the increase in turnover stemming from entering new markets and benefiting from harmonised requirements in EU consumer law.

There are significant benefits to consumers of EU consumer law in terms of ensuring uniform levels of protection within the Digital Single Market. However, the benefits could still be maximised though improve enforcement in the digital environment and better awareness.

There are also however disbenefits for consumers in terms of the persistence of consumer detriment linked to problematic practices, as analysed in detail in the section on detriment within the sub-section on costs and benefits for consumers.

CPAs reported moderate costs of monitoring compliance, relative to the benefits due to the recent changes made through the MD. Nonetheless, they pointed to how recently the MD was applied, and the need for more time before being able to fully assess the impact of the changes on the enforcement activities and resource implications.

However, CPAs reported moderate-to-high costs of applying EU consumer law in the digital environment generally, due to the complexity of applying consumer law with digital and data laws, and the opaqueness of some technologies and design interfaces, which require careful investigation to be able to pursue enforcement actions.

Proportionality focuses on the financial and administrative impact of legislation, to ensure that regulatory actions do not exceed what is necessary to achieve the legislative and policy objectives. Any such impact must be minimised and must be proportionate to the policy objectives, or, in other words, the benefits of meeting these.

A challenge in making a direct comparison between benefits and costs was that whereas the latter can be quantified, the former often cannot. A further challenge was that benefits typically take longer to materialise whereas many costs (e.g. compliance costs) are incurred upfront if they are one-off or on a recurring basis, but before the full benefits are accrued.

Given these difficulties, qualitative feedback regarding the benefits has been used, including their nature and approximate magnitude where this cannot be quantified directly. In addition, some proxy data has been used where appropriate (e.g. assessing the evolution in the size of digital markets and services over time, CCS data on levels of activity among consumers in making digital transactions).

Earlier in the cost-benefit, the findings in respect of the costs for traders were provided based on the enterprise survey. The **adjustment costs** were estimated at between **EUR 208m and EUR303m across the EU but more regular costs arise from checking compliance with the legislation, of the range of between EUR249.8 m and EUR487.5m across the EU, annually. These are based on assumptions spelled out in the methodological Annex.**

Against the costs of the legislation, the following values are reported for the markets considered within this fitness check:

- **European e-commerce sector** - in 2022, the European B2C e-commerce **turnover** increased from €849 billion in 2021 to €899 billion in 2022³⁰³.
- **Platform economy** –the EU's platform economy has grown exponentially from an estimated €3 billion in 2016 to €14 billion in annual revenues by 2020, according to Eurostat data.
- **Subscription economy**³⁰⁴ – research by ING suggests that the average European household spends 130 EUR per month on all subscriptions, for an estimated market worth of 350 billion EUR, 5% of total European household consumption.

Additional costs were reported from the implementation of the MD and some of the disclosure related clauses but the results would appear to be inconclusive (with the enterprise survey noting small costs and the targeted consultation reported higher costs). Several provisions from the MD only applied to online platforms and marketplaces, which could explain the differences in costs between the enterprise and the targeted consultation. The highest perceived costs related to the provision of information on the criteria used for explaining the search result rankings and the verification of online reviews to ensure they are authentic. **The familiarisation costs of providing information** due to new transparency obligations were regarded as **significant** by 35% of respondents and moderate by a further 45%. A contrast can be made between perceptions among traders of low to modest costs of longstanding pre-contractual information requirements in the CRD, whereas relatively high costs of new information requirements in the MD. This validates the finding that one-off compliance costs due to new or recent obligations are perceived as being much more costly compared with regulatory compliance obligations introduced already some time ago. On the other hand, the redesign of websites or online interfaces to provide additional information to consumers due to new transparency requirements entailed minimal to moderate costs.

Overall, the costs of traders of meeting consumer protection related legislation are dwarfed by the values of the digital related economy highlighted above. Although the growth in digital markets cannot be directly attributed to the legislation considered here, it is not unreasonable to expect that some of that increase is also due to the increased protection that legislation is offering consumers which are more trusting.

It can be observed that whilst consumers are sufficiently trusting given that a higher percentage of the EU population make purchases online compared with 2016 data³⁰⁵ (71% compared with 57.8% according to the CCS), they **continue to experience consumer detriment**. The non-optimisation of the digital single market can result in consumers lacking trust in e-commerce websites due to deceptive designs, fake reviews, difficulties in cancelling subscriptions, reluctance to try new products and services due to requirement to provide credit card details. This in turn will affect trade. Effective implementation by CPAs, greater compliance by traders and increased awareness by consumers can all contribute to reduce consumer detriment.

Traders and trade associations were positive about the benefits of EU consumer law. They firstly mentioned the **single market benefits of harmonised legislation** through increased trade (see Section 3.2 on the development of digital markets and services). They did however express concerns about the risk of regulatory fragmentation emerging in some areas due to national legislation. This issue is explored in detail under EQ5 regarding the development of

³⁰³ [European e-commerce continues to grow despite shifting economic environment - EuroCommerce](#)

³⁰⁴ The subscription economy refers to a business model where companies offer their products or services to customers through recurring subscriptions rather than one-time purchases. In this model, customers pay a regular fee (monthly or annually) to access goods, services, or content. Examples include streaming services (like Netflix), software subscriptions (such as Microsoft 365), meal kit deliveries, and even curated product boxes.

³⁰⁵ 2016 was the benchmark used for the indicators and targets put forward in the MD impact assessment 2018 – see <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018SC0096> COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT SWD(2018) 98 final

national legislation on unfair and misleading practices, and how this could risk undermining the single market.

Whilst harmonisation benefits were difficult to quantify, evidently, there would be **significant compliance costs associated with complying with 27 different national sets of legislation**. Regarding stakeholder feedback, evidence was identified of reduced barriers to cross-border digital trade through the maximum harmonisation approach in the UCPD and the CRD.

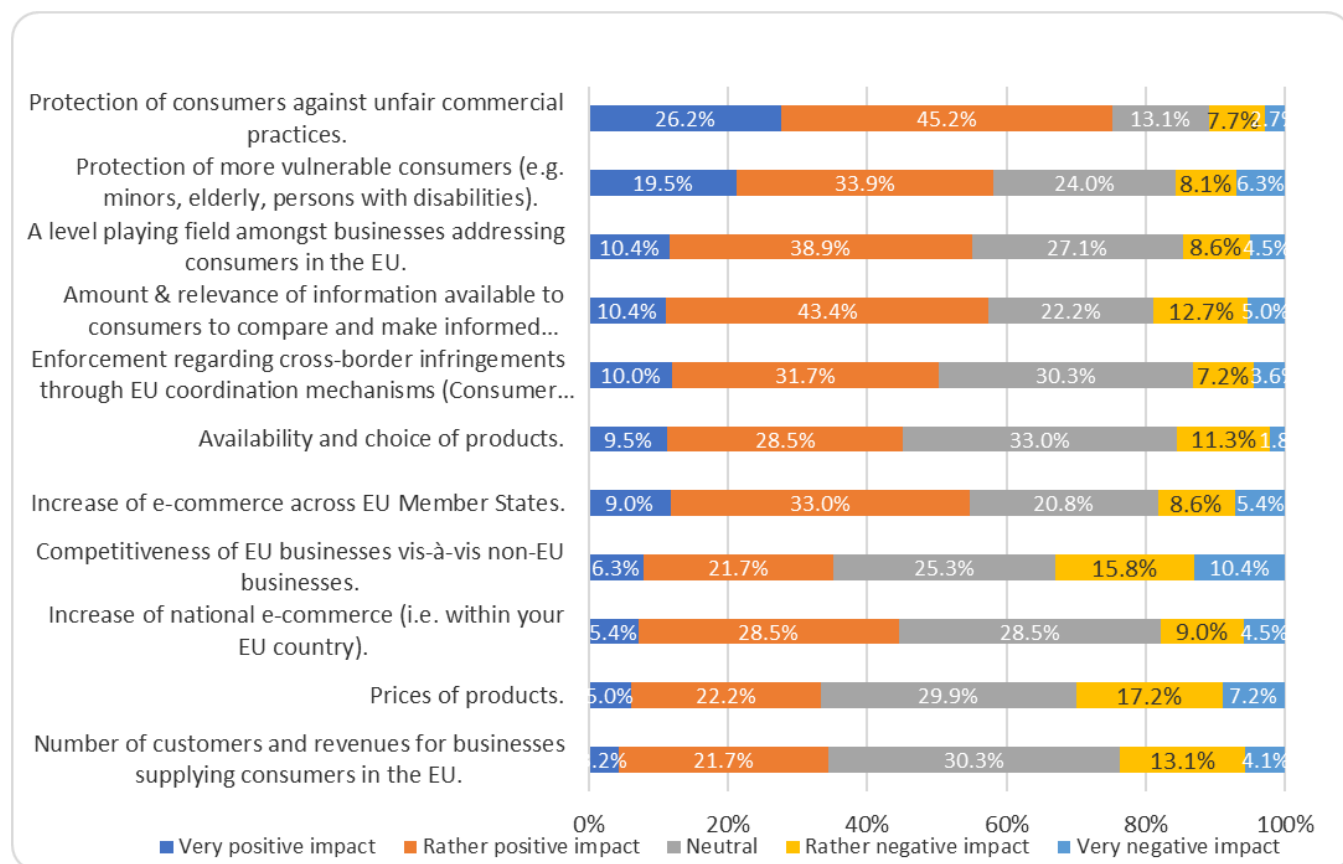
Secondly, benefits relating to **having regulatory certainty** were mentioned. Trader associations observed that the consumer law framework – supported by the Commission’s guidance – is legally clear to a certain extent and this has brought regulatory certainty. They supported the idea of not being too specific with the rules, but rather applying the general principles test and allowing case law to play a role in interpreting the rules as new business practices in the digital environment emerge over time. However, they expressed concerns regarding how the legislative review processes and changes to EU law in the past five years in terms of the effects on the ongoing benefit of regulatory certainty.

EU trader associations representing the digital sphere and individual large tech traders were concerned about the increased frequency of regulatory developments. They said that there were many ongoing legal changes, and consultations on these changes not only in EU consumer law but also in other areas of EU law that interact with EU consumer law (e.g. digital and data law). This was seen as having caused some uncertainty for traders as they are unsure if there will be further changes in future to align consumer law with other regulatory changes.

There are concerns among traders regarding national barriers emerging from the development of national rules for some specific digital practices. These could lead to future regulatory uncertainty, although as noted above, when looked at across the past 20-30 years, consumer law has provided regulatory stability. The concern is that future legal changes and the growing complexity of applying consumer law with other types of law could undermine stability.

Some feedback on benefits was also received through the public consultation (as per the figure below, and the open responses).

Figure 3-26 Benefits of EU consumer law. Question: How positive / negative has the impact of the existing EU consumer law framework been on the following aspects in the digital environment? (n=207³⁰⁶)

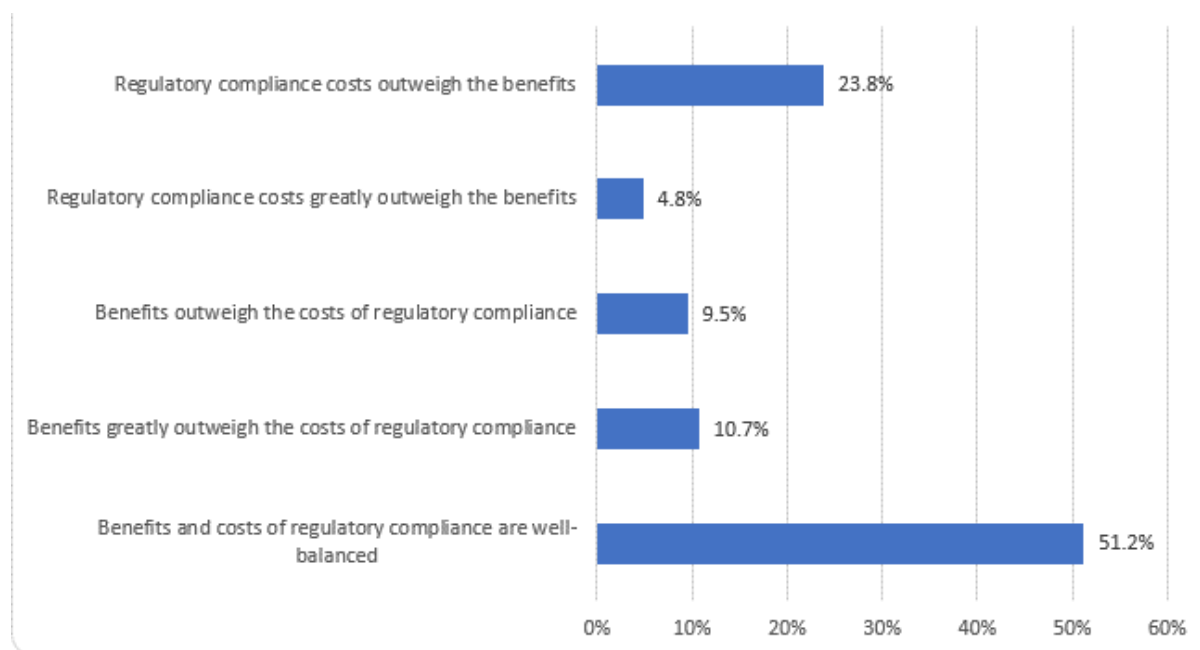


Source: Digital fairness public consultation survey undertaken in November 2022 – February 2023

Mostly, respondents agreed that the benefits and costs are well balanced (although a similar % could not provide an answer), with over 50% stating that the benefits and costs are well balanced. For 22% the benefits outweighed the costs and a similar percentage (28.6%) stated that the costs were larger than the benefits. Others provided more detail in their responses. For instance, eCommerce Europe notes that EU consumer law should have positive benefits through harmonisation in contributing to the growth of ecommerce nationally and cross-border. In a joint study with McKinsey, they estimated that by 2030, ecommerce will double, and 90% of the growth in retail will be online. However, they expressed concerns about the cumulative costs of legislation.

³⁰⁶ Excludes 14 don't knows

Figure 3-27 - 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)



Targeted consultation

As there is a large volume of e-commerce activity and the benefits from increased certainty of the regulatory framework for both consumers and traders, the **benefits of EU consumer law are expected to outweigh the costs**. Benefits could be significantly larger than those that have realised thus far, with increased consumer awareness of rights and improved implementation, enforcement and compliance by traders more generally.

3.2.7 Opportunities for simplification

EQ6(5) – Are there opportunities to simplify the legislation or reduce unnecessary regulatory costs without undermining the intended objectives of the Directives?

Overall, given that existing EU consumer law rules are necessary to ensure that commercial practices and standard contract terms are not unfair, there appears to be limited scope for simplification in the digital environment. However, some suggestions were made by consultees as to possible ideas on simplification. These mainly related to:

- Reducing the volume of information provided to consumers that was burdensome.
 - Reducing pre-contractual requirements for e-commerce traders - which were deemed to be too onerous by some traders and duplicated between the CRD and the UCPD. However, the scope to eliminate requirements has already been explored through the MD IA.³⁰⁷
 - Reducing the overall volume of disclosures. Whilst the new disclosures in the MD do not appear to be burdensome, some stakeholders (and even consumer associations) identified too many disclosure rules across different pieces of EU law (e.g. including the DSA, national consumer rules) and this information realistically is not being read by consumers).

³⁰⁷ However, this perceived duplication was already explored in the Modernisation Directive impact assessment study and in the guidance. The pre-contractual information to be provided by traders may be similar or identical but it relates to different stages in the transactional process, thereby minimising the scope for simplification. Moreover, consumer organisations responding to the consultations did not want pre-contractual information requirements to be reduced.

- Requiring traders to produce a simplified overview of terms and conditions detailing key points, but leaving out pages of legal jargon.

The extent to which there are opportunities for simplification was considered through the study, building on earlier efforts in the 2017 Fitness Check to investigate this issue, but with a focus on the digital environment.

The 2017 Fitness Check assessed the potential for rationalisation to improve the coherence and to simplify the current regulatory framework such as to reduce regulatory costs and burdens including administrative burdens, while guaranteeing a high level of consumer protection.

In the public consultation, stakeholders considered that there is some scope for simplification and burden reduction in existing EU consumer laws (26% strongly agree and 38% agree). The following figure shows the result of our targeted survey on the possibilities of simplification³⁰⁸. Results shows that nearly 40% considered that there was significant scope for simplification and a further 31% considered that there was some. Among the responses, the following suggestions can be highlighted:

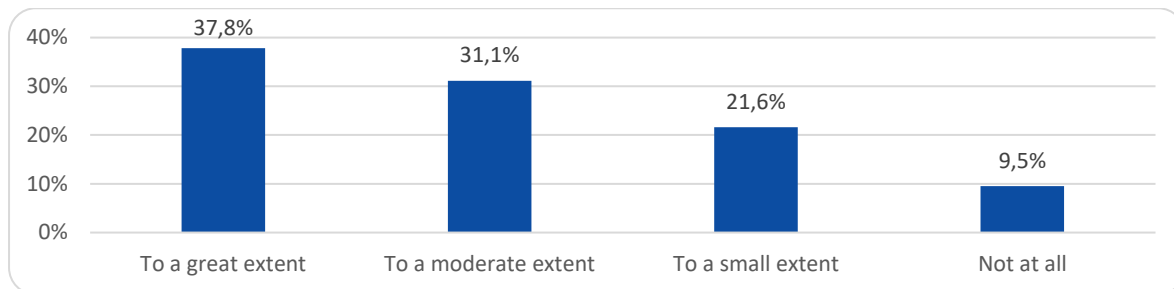
- Reducing information obligations given the information overload on consumers due to extensive transparency requirements both in EU consumer law and in other applicable laws, such as the DSA);
- Whilst the rules currently apply to all traders (digital and offline), an exception is that there are some more specific rules for platforms introduced through the MD. Some stakeholders would favour extending rules applicable to platforms to all traders.
- SMEs and some large firms also found it challenging to keep up with continuous legal amendments and new legal proposals (an example being the UCPD, CRD and Circular Economy Package). Reducing obligations for SMEs, especially pre-contractual information requirements was therefore suggested. However, a disadvantage of this approach would be that consumers would lack relevant information to make informed decisions in some circumstances, but would receive adequate information from large and multinational firms which could undermine the level playing field.
- Removing the RoW for digital content that is instantly provided and/or consumed. Some stakeholders saw it as not being helpful if consumers are given a theoretical right but then have to agree to waive it to consume the product.
- Allowing more self-regulation rather than legislation. This however could introduce differences in implementation if voluntary approaches are not consistently applied by industry, and thus increase uncertainty and affect consumers' trust.
- Simplification of the rule on price promotions to enable traders to make genuine price reductions at regular intervals (i.e. the regulatory option foreseen for successive price promotions should be generalised to the EU). Further guidance on how to calculate average prices and a reference price (given the frequency of price changes in some sectors) for the previous 30 days would help provide clarity and save resources for traders.

Another respondent added that: *“Amending EU Consumer Law every few years because there is a new online practice is not effective. Digital innovation evolves quickly and it is unrealistic that the current ad hoc and detailed approach of EU legislators is sufficient. It is probably more effective to strengthen the principle-based approach and horizontal nature of relevant EU Consumer Law. Specific issues could still be regulated in sector-based regulation. Also,*

³⁰⁸ Q57: to what extent are there opportunities to simplify legislation or reduce unnecessary costs?

developing new legal requirements without strengthening enforcement is meaningless. Consumers are not better protected and traders that do their best to be compliant with the new rules are losing ground due to rogue traders that will ignore any new rules by default.”

Figure 3.28 – To what extent are there opportunities to simplify the legislation or reduce unnecessary regulatory costs without undermining the objectives of the three EU consumer law Directives (i.e. CRD, UCTD, UCPD) in the digital area? (n = 74)



Regarding the suggestions made by stakeholders to simplify the legal framework, caution is needed, for instance in relation to avoiding undermining a high level of consumer protection by reducing information provision to consumers (even recognising that a significant percentage do not read the information), given the need to ensure high levels of consumer protection. The risk of unintended consequences should not be overlooked either. For instance, traders and trade associations interviewed pointed to a seemingly beneficial idea such as producing a simplified overview of terms and conditions detailing key points for consumers carries risks. Whilst there would be a benefit for consumers that key information would be more useful compared with pages of legal jargon in T&C, traders were concerned that all the detail is still necessary, and they could risk complaints and legal cases for points overlooked in the simplified T&C.

3.2.8 Summary assessment of the costs and benefits of EU consumer law in the digital environment for different stakeholders

The costs of compliance with the Directives were analysed drawing on the limited quantitative costs data provided by traders and their representative associations through the enterprise survey (and where questions were included, also from the targeted and public consultations), complemented by a review of previous evaluations and other studies to obtain any benchmark data. Some data on non-compliance was also obtained based on survey feedback and the results from CPC sweeps and the sweeps undertaken in this study. Some qualitative feedback on compliance costs was obtained through the targeted and enterprise survey undertaken as part of this study. The main findings show that:

- A few traders experienced significant one-off costs to do with familiarisation. However, as most of the applicable laws have been in place for a considerable time period, administrative and adjustment compliance costs were mainly incurred a long time ago, given that the Directives were adopted in 1993 (UCTD), 2005 (UCPD) and 2011 (the CRD). Traders are therefore already strongly familiar with the information requirements and their compliance obligations.
- However, exceptions were newer familiarisation costs linked to regulatory amendments due to new changes introduced recently through the transposition of the MD into national laws coming into application from May 2022. There will still be familiarisation costs as new businesses get created in dynamic digital markets and services sectors. Moreover, there are also such costs incurred by traders operating online only as they will have to familiarise themselves with all applicable legislation

(whilst traders operating in multiple channels are likely to incur significantly smaller costs).

- Traders in the digital environment will also experience some recurring costs, for instance, in relation to the updating of Terms and Conditions (T&Cs) given they will have to check compliance with the UCTD. In addition, there will be some adjustment costs from having to redesign processes or websites to ensure compliance with the provisions (e.g. general provisions that cover many different digital practices such as dark patterns, hidden ads). However, the consultations have suggested that these costs are not significant (provided that compliance is designed in from the outset).
- Consumers were found to still experience considerable detriment when conducting transactions in the digital environment, despite several additional new protections introduced through the MD to improve transparency and prohibit certain practices. Ongoing detriment was found to be due to the persistence of problematic practices. There were to be found to be ongoing problems with poor compliance by some traders with existing provisions and a lack of enforcement, and a lack of awareness about consumer rights and/or bad practices that remain among traders.
- It is not possible however to say whether this is attributable to the deficiencies in the regulatory framework alone. Consumer detriment is not, however, expected to be commensurate to the benefits experienced by consumers when buying online (in terms of choice and price of goods). The benefits cannot be measured with accuracy but the stakeholder consultations (interviews, surveys) provided strong evidence that the application of consumer law in the digital environment has delivered major benefits to consumers (uniform protection through harmonised laws) and to traders (single market benefits) due to the three directives' implementation. However, there is still scope for improvement in many problematic areas to reduce detriment in future.
- Competent authorities and CPAs revealed that the most significant costs are related to checking that traders are compliant through inspections conducted in the digital environment (e.g. of websites, apps, platforms, marketplaces and of AI systems and algorithms). The benefits for these stakeholders are related to reduced legislative uncertainty compared with relying on guidance alone and potentially contributing to improved compliance by traders in future, given that clearer rules for the digital age such as those recently introduced through the MD, will better enable CPAs to take action and to issue enforcement notices to potentially non-compliant traders to deter non-compliance. This may result in a reduction in CPAs' legal costs of bringing traders to justice. No specific estimates have been made available.

3.3 Relevance

According to the 'Better Regulation Guidelines', an evaluation should look at the objectives of the EU intervention being evaluated and see how well they (still) match the (current) needs and problems. Relevance can be defined as the extent to which the EU consumer law framework addresses identified needs at a regulatory level relating to achieving the Directives' general and specific objectives and the needs of its target group(s), especially consumers and traders. In a fitness check context, under this criterion, the focus was on assessing whether the legislation demonstrates ongoing fitness for purpose in being able to deliver digital fairness, including its ability to adapt to emerging developments and trends in digital markets and services.

Assessing the relevance criterion had a forward-looking dimension, given developments in digital markets and in EU legislation impacts on the consumer law framework's ongoing and future likely relevance. The interconnected nature of relevance and coherence should also be

stressed, as major developments in the EU legal framework overall, especially through recent digital and data laws impact on EU consumer law.

3.3.1 Relevance to identified needs

EQ8 – To what extent do the Directives remain relevant and correspond to the identified needs of consumers and traders? How far does the legal framework remain fit for purpose in addressing digital asymmetries faced by the average consumer?

Overall, the Directives' objectives and key provisions relating to the prevention of unfair commercial practices and unfair contract terms were found to remain relevant to addressing the identified needs of consumers (ensuring high levels of consumer protection in the digital environment) and to traders (in a digital single market context). However, to ensure ongoing relevance, and to be able to deliver digital fairness in future, there **could be a need for more specific rules in certain areas to strengthen the regulatory framework's capacity** to address different trends and developments, such as:

(1) The wide variety of different business practices by traders in digital markets and services, some of which are perceived by consumers, consumer associations and CPAs as being problematic.

(2) The increasing diversity of traders in digital markets and services and wide heterogeneity of digital environments in which transactional decisions take place. For instance, the CRD (adopted 2011) was designed at a time when B2C e-commerce was still evolving. The UCPD, adopted in 2005, was drawn up prior to the data economy becoming a central feature of the European digital economy and prior to the advent of the platform economy. Today, there are many more types of traders active in the digital environment than when EU consumer laws were drawn up (e.g. platforms and marketplaces, influencers, etc.).

(3) Increased use of screenless connected devices in an IoT and smart home context, which has implications, e.g. medium for provision of pre-contractual information.

The above developments have implications for the ongoing fitness for purpose of the EU consumer law framework. As explored under EQ10 (ability of consumer law to be flexible enough to accommodate new technologies and digitalisation), if EU consumer law is to remain relevant and future-proof, reflection is needed whether the body of EU legislation can continue to be pertinent given **digital asymmetries**, which have become more pronounced due to the complexity and opaqueness of digital technologies, such as the use of AI and algorithms.

A combination of **societal and technological developments may mean revisiting whether the existing framework is sufficiently technology-neutral**. For instance, in the context of trends such as smart homes, increased use of screenless connected devices in an Internet of Things (IoT) context means that consumers are making transactional decisions that do not allow pre-contractual information to be easily provided. There may not be a screen on the voice-activated IoT device directly. Likewise, it could be difficult for traders to include an 'obligation to pay' a specific price via a button. Flexibility will therefore be needed to ensure ongoing technology-neutrality e.g. emailing of pre-contractual information when not visible on a particular device, voice confirmation that consumer understands and agrees to the final purchase price, etc.

This EQ focuses on the overall perceived ongoing relevance of the consumer law framework from a digital fairness perspective and considers the views of both consumers and traders. Generally, the legal framework was perceived by stakeholders in the various consultations as being broadly fit for purpose, but with some outstanding questions raised under the effectiveness section as to whether given the nature and extent of digital asymmetries faced by the average consumer, the legal framework can remain relevant in ensuring consumer protection without more specific rules in some areas to mitigate the problem of digital asymmetries, which were explained in Section 3.1.2 – Key concepts in framing the fitness check. The relevance of the legal framework may be undermined as legal protections to address asymmetries focus on the notion of the average consumer but without taking into full

account the extent of digital asymmetries and their impact on the balance in transactional decisions between traders and consumers. Some position papers have strongly stressed that **situational vulnerabilities in the digital environment** could influence transactional decisions and lead consumers to make purchases they would not otherwise have made, necessitating an updated definition. This is explored in EQ4(2) on transactional decisions and under problematic practices (subscription traps, dark patterns and other aggressive practices).

From a trader perspective, stakeholder feedback from interviews was that the legal framework remains relevant and the general principles-based approach allows flexibility to accommodate new technologies and digitalisation as well as to allow for the evolution in new business practices as these can be addressed in the guidance. However, as noted earlier under effectiveness, problematic practices remain common, and levels of enforcement not as high as both consumer and some trader associations would prefer. The perceived lack of adequate enforcement could risk undermining ongoing relevance without more specific rules, according to consumer associations, CPAs and some Ministries interviewed and responding to the public and targeted consultations.

The Directives' objectives were considered broadly relevant to addressing consumer needs in the context of the challenges created by the evolving digital environment in which consumers face digital asymmetries, thereby widening the number of potentially vulnerable consumers beyond the traditional definition of a vulnerable consumer in Art. 5(3) of the UCPD. A more detailed assessment of fitness for purpose in addressing consumer vulnerabilities is provided in EQ9 in the next question.

As highlighted in several EU-wide studies including the Commission's 2016 study on "Understanding consumer vulnerability in the EU's key markets", a 2018 consumer survey on self-perception of vulnerability, and the 2019 Consumer Conditions Scoreboard, increasingly large segments of the EU population consider themselves to be vulnerable. For instance, in 2019, 43% of EU citizens surveyed believed themselves to be vulnerable consumers for one or more reasons (mainly linked to their socio-demographic status, and the complexity of offers, terms and conditions, etc.). The percentage of self-reported vulnerable consumers was 35% in 2016 indicating a growth in perceived vulnerability among consumers. This is in line with the findings from academic literature, consumer reports and the feedback from all stakeholders consulted as part of the vulnerable consumer case study, which highlighted increased consumer vulnerability due to the evolving digital landscape.

The fast pace of the digitalisation of the consumer landscape was noted by BEUC in its 2021 "EU Consumer Protection 2.0" study which suggests that due to large parts of consumer activities moving into online space and onto digital platforms, the average consumer has now become a vulnerable consumer. This is also in line with the findings of the New Consumer Agenda which highlights that the digital transformation – together with the underlying data collection, processing and analysis of consumers' behaviour and their cognitive biases – can make it harder for all consumers to make informed choices, and may limit the effectiveness of the current rules, including on unfair consumer practices. For instance, some practices could lead to increased consumer vulnerability, such as the use of user interfaces aimed at manipulating consumers, abusing consumer behavioural biases, profiling, hidden advertising, false or misleading information and manipulated consumer reviews. This are delved in further details as part of the case studies.

Regarding the relevance of the Directives' objectives to addressing identified policy needs and stakeholder needs, as explained under effectiveness, the three Directives place a strong focus on achieving a high level of protection for consumers and on fostering an effectively-

functioning single market in parallel. These core objectives of EU consumer law were considered to remain relevant by stakeholders consulted, as now explored:

- **High-levels of consumer protection** – confirmed by all stakeholders. It remains important to ensure consumer trust in the digital environment, given the increased importance of digital markets and services to the European economy.
- **A (Digital) Single Market with free movement of digital goods, services, and content.** From a trader perspective, EU consumer law provides a maximum harmonisation framework in the case of the UCPD and CRD that remains relevant to facilitating intra-EU trade, whilst protecting consumers, and crucially avoiding 27 different national sets of consumer law applicable in the digital environment.

Stakeholders reported that the Directives’ objectives are still valid today. However, whilst considered increasingly relevant for the protection of an increasing number of (more) vulnerable consumers, some stakeholders did not think that the provision enacting the objectives were sufficiently precise enough to ensure they are interpreted in the same way across all Member States. This issue was raised and discussed highlighted in EQ3 on the extent to which the Directives were successful in achieving their objectives.

3.3.2 Relevance to addressing the needs of vulnerable consumers in a digital context

EQ9 – How far has EU consumer law remained relevant in addressing the needs of vulnerable consumers in the digital environment?

Further sub-questions considered were:

EQ9(1) – To what extent is the existing concept of ‘vulnerability’ defined in the UCPD still relevant?

EQ9(2) What role does the concept of an ‘average consumer’ play in the digital environment and in the evolution in what constitutes a vulnerable consumer?

By treating the vulnerable consumer as an exception to the (rational) average consumer, the UCPD does not consider the fact that vulnerability may concern a much larger proportion of the population, nor does it consider the notion that all consumers may experience vulnerability in the digital age (given digital asymmetries and situational vulnerabilities in which all consumers may potentially be vulnerable in specific circumstances).

As noted by stakeholders consulted for the vulnerable consumer case study, amending the definition of a vulnerable consumer in the UCPD’s Art. 5(3) to include a more flexible conceptualisation of vulnerable consumers would allow for a wider range of vulnerabilities to be included and legislated for, thereby increasing the relevance and use of the vulnerable consumer concept.

There is a need for further Commission guidance and a potential role for non-mandatory industry guidelines for traders on how to ensure that consumer vulnerability is taken into sufficient account in a digital context, including as regards how to ensure that digital fairness by design principles are adhered to with particular attention to the needs of specific vulnerable groups, such as children and minors.

The definition of consumer vulnerability is quite broad in some areas, such as the UCPD’s reference to age only, without mentioning the importance of ensuring adequate protection of children and minors’ rights

Addiction-related vulnerabilities are also not addressed in the current definition, but recent 2023 work by the EP’s IMCO Committee found that digital addiction is a significant societal and mental health-related problem, with children particularly affected.

If children were to be more explicitly referenced, a standardised approach to defining age would be needed. Given that children have a lack of personal and legal autonomy, obtaining redress through

complaints and enforcement is less accessible. Therefore, consideration could be given to a possible reversal of the burden of proof in certain circumstances where representatives of minors would find it difficult to establish a sufficient evidential basis to take action. Representative actions could also contribute towards a solution in this regard (e.g. when groups of consumers come together to obtain redress).

This EQ addressed the extent to which EU consumer law has remained relevant in addressing the needs of vulnerable consumers in the digital environment, including an assessment of the pertinence or conversely outdatedness of the definition of what constitutes a ‘vulnerable consumer’ and whether the focus should continue to be on individual characteristics or if a more holistic approach is needed that recognises situational vulnerabilities.

The average consumer, digital vulnerability and the extent of digital asymmetries

In Section 1.4, the concepts of an average consumer and a vulnerable consumer were introduced. Some feedback from stakeholders on these notions was obtained. The concept of the average consumer has been clarified in CJEU rulings and defined in the UCPD’s Article 5(2). An average consumer is a consumer who is “*reasonably well-informed and reasonably observant and circumspect*”, whereas the concept of a vulnerable consumer relates to their personal characteristics and has been defined in narrow terms (i.e., age, infirmity, credulity).

Some stakeholders argue that the concept of an average consumer has become outdated and is no longer as relevant in the context of the digital environment. All consumers can be vulnerable in certain situations, regardless of whether they meet the definition of a vulnerable consumer.³⁰⁹ Users of digital content and services may also face a situation in which they have more limited choices due to design architectures without them necessarily being aware that the choices they are presented with may be down to interface design architectures. Here, the concepts of structural and architectural asymmetry in the choice architecture of the service and access to data are relevant.

A more accurate representation of the average consumer is the “disengaged consumer” identified in the European Commission report on consumer vulnerability as a category of consumers who fail to read terms and conditions, is unaware about their contract terms and conditions or does not read communications from their providers. Consumer experts such as Siciliani, Riefa and Gamper have highlighted how ‘disengaged’ consumers find themselves in vulnerable purchasing situations, not because of “cognitive failings or sociodemographic characteristics”, but because of the “structure of the consumer markets on which they evolve leads to apathy through obfuscation”.

The concept of digital asymmetry is again helpful, as the average consumer does not understand how AI systems and algorithms that drive digital services, such as platforms influence choice architectures. Moreover, whilst transparency obligations are helpful for consumers, such as whether a price has been personalised, whether a decision has been made using automated decision-making, alongside lengthy T&Cs, they can lead to information overload (in a similar way to the longstanding problem of cookie fatigue regarding the collection of personal data), exacerbating information asymmetries.

Some Ministries and CPAs, but also some trader associations recognised that digital asymmetry is different from conventional informational asymmetries and the traditional power imbalance between traders and consumers. However, some legal academics noted that whilst there can be digital asymmetries, informational asymmetries are less of a problem in the digital

³⁰⁹ See case study on consumer vulnerability for bibliography and for an introduction to the topic, EP briefing paper, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690619/EPRS_BRI\(2021\)690619_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690619/EPRS_BRI(2021)690619_EN.pdf) and BEUC position papers on the topic of consumer vulnerability, such as: EU CONSUMER PROTECTION 2.0 - https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf and The manipulated consumer, the vulnerable citizen - https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-075_the_manipulated_consumer_the_vulnerable_citizen.pdf

environment than offline (e.g. as personal virtual assistants, price comparison websites and search engines can provide consumers with quick access to extensive and easily comparable information). However, this presupposes that consumers have basic digital skills whereas vulnerable consumers (e.g. the infirm and elderly), may benefit less from such tools if they lack such skills.

Consumer vulnerability and the definition of ‘vulnerable consumers’ in the UCPD

The UCPD is based on the idea that, while it is appropriate to protect all types of consumers from unfair commercial practices, ‘vulnerable consumers’ who qualify as members of one of the groups listed in Article 5(3) (i.e., age, infirmity and credulity) should be ensured a higher level of protection than ‘the average consumer’ referred to in Article 5(2). The UCPD approach thus emphasises a limited set of individual characteristics that increase the (theoretical) risk of becoming vulnerable. While this approach offers legal certainty as to who should be considered vulnerable and is therefore easier to legislate for, it does not account for the wide array of potential vulnerabilities that consumers may face (i.e., such as low socio-economic status, low education level, not being able to speak a particular language, a minority status, etc.).

Regarding how effective and relevant the concept of consumer vulnerability is, beyond the limited set of vulnerable groups listed in the Directive presently, experts have also criticized the approach of identifying specific groups of consumers. This is what Cole calls the “victim approach” to vulnerability, as the concept is used to draw attention to the inherent weakness of particular groups, or their inability to fend for their own interests. Similarly, Martha Fineman argued in her vulnerability theory³¹⁰ that consumer vulnerability is not a fixed characteristic but a consequence of human embodiment, carrying with it “the ever-present possibility of harm, injury, and misfortune” and therefore “no individual can avoid vulnerability”. This is particularly relevant when it comes to the digital environment where all consumers can become vulnerable. The notion of “vulnerability by default” (and the related “digital asymmetry” also highlighted by BEUC) have previously been discussed. These are further elaborated upon in the case study on consumer vulnerability in the digital era.

While acknowledging the trade-off between legal certainty and a broader definition of vulnerability, there was consensus among the consumer experts consulted that a broader definition within the article was desirable to broaden the categories of vulnerable consumers and align the text of the article with the intent of the Commission (as per the UCPD guidelines and study³¹¹). As highlighted by one national authority interviewed: “It is only after the term is defined that an effective regime of protection can be set up, which is not the situation at present.” While the UCPD’s Recital 19 and the Commission’s guidance documents on the implementation and application of the UCPD suggest that the closed list of vulnerable groups in Art. 5(3) may not be exhaustive (by adding “such as” before the list), to date, few courts have extended the scope of this notion past the list contained in the article. Using recital 19 to interpret Art.5(3) UCPD might result in conferring rights to consumers who might otherwise not enjoy them as per the law. Given that the UCPD is a maximum harmonisation directive (i.e. it sets both the minimum floor and a ceiling of protection) Member States cannot deviate from the UCPD standard to protect vulnerable consumers such as by having stricter or more comprehensive standards of protection for certain groups. This may explain why Member States have taken the safer approach of limiting the interpretation of the Directive to the group of vulnerable consumers listed in the Articles of the Directive.

Moreover, beyond the debate regarding which additional vulnerabilities should be included in the UCPD definition of vulnerable consumer, findings from the vulnerability case study also

³¹⁰ ‘The Vulnerable Subject: Anchoring Equality in the Human Condition’ in the Yale Journal of Law and Feminism (Fineman, 2008).

³¹¹ European Commission, 2016, Understanding consumer vulnerability in the EU’s key markets, Available at: [Understanding consumer vulnerability in the EU’s key markets \(europa.eu\)](https://ec.europa.eu/consumers/odr/files/understanding_consumer_vulnerability_in_the_eu_s_key_markets_en.pdf)

suggest that the concept of the “vulnerable consumer” is difficult to prove and use in practice due to the restrictive elements that need to be met (i.e. the consumer needs to be part of a clearly identifiable group of vulnerable consumers; the malpractice should only target the individuals within that group; and the trader could not have reasonably foreseen that harm would be caused to that particular group by the practice). The restrictions and difficulties in the application of the vulnerable consumer concept (see vulnerable consumers case study for detail) are among the reasons why it is rarely used by national enforcement authorities and the courts, and why the ‘targeted average consumer’ is often used for the protection of the vulnerable consumers instead. Because the targeted average consumer standard is more flexible, in that it can refer to any group, it has allowed for better protection of vulnerable categories than the vulnerable consumer concept. Moreover, as infringements/malpractices targeted at vulnerable consumers are treated the same as those targeted at the average consumer, there are no perceived benefits for consumers or regulators to use the more rigid dan narrow vulnerable consumer concept.

While stakeholders consulted did not consider that an issue as the average targeted consumer standard can effectively be used to protect vulnerable consumers, it brings into question the relevance of the vulnerable consumer concept if the concept is not broad/flexible enough (in terms of the scope of categories of vulnerable consumers) or applicable (in terms of the requirements it sets) to be used. The limited set of vulnerable groups listed in the UCPD and CRD is restricting the extent to which vulnerable groups are named and considered and thus protected. All stakeholders consulted as part of the vulnerable consumer case study (consumer groups and experts) suggested broadening the definition and expanding the characteristics.

By treating the vulnerable consumer standard as an exception to the (rationale) average consumer, the UCPD does not consider the fact that vulnerability may concern large parts of the consumer population or the notion that all consumers may experience vulnerability in the digital age. While the 2021 UCPD guidance documents introduced the concept of vulnerability in the digital environment highlighting that consumers are particularly vulnerable on online markets, no changes were introduced to the UCPD which still benchmarks the vulnerable consumer against the outdated (defined in 1996) rational average consumer.

This case is further developed by BEUC which argues that the digitization of consumer markets and electronic transactions has introduced new forms of personalized persuasion strategies that can be directed, very purposefully, at making all consumers vulnerable, as they are not able to rationally deal with a particular marketing practice. The growing power imbalance between the traders and the consumers (i.e. digital asymmetry) results in a universal state of vulnerability for the consumers, referred by BEUC as digital vulnerability whereby traders control information presented to the consumer, and the entire choice architecture (i.e. nearly all services that consumers encounter in the digital environment benefit from insights formed by detailed knowledge of their online searches.)

As noted by stakeholders consulted for the vulnerable consumer case study, amending the terminology of the UCPD to include a more flexible conceptualisation of consumer vulnerability would allow for a greater range of vulnerabilities to be included and legislated for, thus increasing the relevance and use of the vulnerable consumer concept.

There was also stakeholder feedback related to the fact that applying the current definition of a vulnerable consumer to their business practices can pose challenges. For instance, the definition includes a focus on physical and mental infirmities, but traders themselves are prevented from collecting sensitive data about consumers so therefore, at the level of dealing with individual consumers, it was seen by some trader associations and traders as being difficult to implement the concept of consumer vulnerability in practice, as they design a one-size-fits all interface, albeit with accessibility requirements designed in.

A comparison with the regulatory approach to protecting consumers between consumer law and digital law can be made. The definition of a vulnerable consumer in the UCPD's Art 5(2) focuses on several different personal characteristics, whereas the DSA does not define consumer vulnerability but affords some additional protections not included in the UCPD. For instance, users of platforms have greater control over personalised advertising and the use of sensitive data for personalised advertising is explicitly prohibited.

Some stakeholders pointed to gaps in the current definition of consumer vulnerability as these over-focus on specific personal characteristics, such as age, incredulity and physical or mental infirmities, whereas vulnerability is multi-dimensional. Moreover, the definition is vague in some areas, such as age, and coverage of physical and mental infirmities, but not explicitly covering minors and people with disabilities. The current definition was found to be an outdated way of considering the nature of consumer vulnerability. Moreover, adequate connections are not made between EU consumer law and equality and non-discrimination related matters in terms of access to digital services. Given progress made in the digital environment through the European Accessibility Act (EAA) in strengthening accessibility of online services for people with disabilities, arguably more could be done in this regard. The EAA will become law in all EU member states in June 2025.

Whilst Art. 5(2) covers age as a dimension of vulnerability, it remains ambiguous what this means and what protection this affords either children and minors or the elderly. There is inadequate attention to protecting minors (including children) within the definition of a vulnerable consumer, a challenge observed in some position paper responses to the public consultation (e.g. from Ministries and CPAs, especially in Scandinavia and the Netherlands) and during interviews with similar stakeholders. It was argued by these stakeholders that it is essential to **strengthen protection of minors more explicitly** as they face vulnerabilities in the digital environment. For example, they may lack the same level of awareness about consumer choice and children and teenagers are at greater risk of digital addiction.

In the Danish Government position paper response to the public consultation, for instance, it was noted that there was particular concern around *"the protection of minors and harmful commercial practices in the digital environment that do not take into account the vulnerabilities of young consumers. With regards to gaming and social media, the emergence of virtual currencies, in-app micro-transactions and loot boxes offers new challenges to ensure consumer protection online. Persuasion techniques and personalization are also prevalent in videogames. The legal framework should therefore also be clarified with this sector in mind"*.

The importance of introducing age verification systems was stressed in some interviews, for instance by a Danish business association as a means of ensuring that minors who are more vulnerable are not exploited in the digital environment.

Stakeholder feedback on consumer vulnerability from the online surveys

In the public consultation, 51% of respondents supported adapting the legal benchmarks of an 'average consumer' or 'vulnerable consumer' to better reflect the actual behaviours of consumers in the digital environment. However, in the targeted stakeholder survey, over half of respondents, primarily representing traders and business organisations, agreed that the Directives **appropriately provide for the concepts of the average consumer and that of vulnerability across various situations and groups**. Over half also considered that the Directives place sufficient focus on accessibility issues for users lacking in basic digital skills, or people with disabilities that could hinder their user-experience and leave them exposed to threats that may have been mitigated against for users without the same impairment or vulnerability. On this third statement, it is worth also noting that of all 121 targeted stakeholders that were asked about accessibility issues, 20.7% responded that they did not know, due either to lack of sufficient information to provide an answer or perceived irrelevance.

Looking at the targeted survey responses by stakeholder type, **traders and business associations are overwhelmingly represented across these statements as the respondents that are most content with the current Directives**. For example, regarding the third statement, that ‘The directives place sufficient focus on accessibility issues for certain types of users’, business associations and traders constitute 20 (76.9%) of the 26 respondents whom ‘strongly agree’. Conversely, **9 (75%) out of 12 consumer associations responded that they either disagreed or strongly disagreed with the statement**. Furthermore, of the aforementioned 20.7% (n=25) respondents who answered ‘don’t know’ in relation to the adequacy of the Directives in addressing accessibility issues, 16 represented business associations (**representing 29.6% of all respondent business associations**) with a further two being traders.

Conversely, only one consumer association and one national ministry, respectively, responded that they were unable to answer. It can be inferred from this stark data that businesses, or at least business associations representing SMEs and other firms, are either content with the regulatory *status quo* (possibly wary of further regulatory burden) or by their own admission they are insufficiently engaged or informed in relation to user accessibility issues to the extent that they cannot provide a response.

3.3.3 Relevance of EU consumer law to new technological and/ or market-related developments

EQ10 – Are there any technological and/ or market-related developments that are likely to challenge the ongoing relevance of the Directives in future? Are there any technologies that could help to strengthen consumer protection?

While differences in perceptions exist regarding the impact new technologies will have on the relevance of the EU’s consumer law framework, all stakeholders recognised the importance of maintaining a **technology-neutral and channel-neutral approach to ensure future-proofing**, as well as the value of a general principles-based approach.

Nonetheless, some stakeholders advocated that there was a need to **adapt and strengthen consumer law to address specific challenges in the digital environment**. These include the deeper imbalances that persist between traders and consumers due to digital asymmetries, for instance due to information and structural asymmetries, the usage of AI systems and algos which are opaque technologies from the perspective of the average consumer, and the corresponding lack of ability of individual consumers and CPAs to understand and/ or investigate practices (e.g. recreating personalisation scenarios).

In an **IoT context**, regulators and traders need to recognise there is likely to be growth in smart devices, screenless devices and in voice-activated purchases with smart devices that were not previously used to conduct transactions playing an increasing role. Traders are already required under the CRD to provide pre-contractual information to consumers and would need to do so via alternative means such as providing information by email in parallel in instances where it could be difficult or infeasible for consumers to read such information on the device itself.

The **use of AI** poses certain challenges and risks for consumers, some of which have already been addressed by regulators e.g. the MD includes an information disclosure requirement if personalised pricing has been determined by automated decision-making, including through AI tools. However, digital asymmetries in AI systems and algos have not been addressed yet. The AI Act provides useful regulatory solutions to address any informational and technological asymmetries faced by consumers and could potentially be

replicated in EU consumer law.

The **use of smart contracts** poses challenges arising from the nature of blockchain given that DLT technologies require an irreversible ledger, making it difficult to reverse contracts, should EU consumer law rights be exercised by e.g. exercising the RoW, as well as leading to concerns related to the accessibility and comprehension of the terms coded in machine language by the consumer, or the risk of disparity between the actual agreement and the coded terms.

New virtual/augmented reality environments (metaverse/immersive technologies) were seen as being unaddressed in EU consumer law presently. Whilst various current legal provisions may apply analogously to contracts and practices regarding these technologies or performed through or with these immersive technologies, there are no specific provisions for the protection of consumers in relation to new virtual/augmented/immersive reality environments.

EU legislation includes different means of ensuring consumer protection in the context of different technologies. Legislation that is not considered 'consumer law' can nevertheless provide for safeguards and solutions that can have a positive impact on consumers' protection level. For instance, the AI Act regulates higher-risk AI systems and places importance on AI being both explainable and ethical, which helps to avoid exploitative profiling using AI. The Data Act provides users of connected devices or related services with a right to access product data and related service data. Or, inter alia, the DSA establishes a framework of due diligence obligations for online platforms that will also benefit consumers.

This EQ is tackled from a strategic perspective in terms of how technological developments in digital markets and services may already be affecting and could affect in future the application of EU consumer law and its ongoing pertinence. Under external coherence, we then consider the interaction between EU consumer law and other types of legislation, including digital laws. In line with the principle of technology-neutrality, digital laws address group of problems raised by technological phenomena. Whilst the AI Act focuses on specific AI-related technologies, most other pieces of EU law do not focus on specific technologies, but rather types of economic operators, such as the coverage of platforms, very large platforms in the DSA and the focus in the DMA on "gatekeepers" in the digital sector, which include large search engines and large platforms. Reference should also be made to Table 4.4 – Interaction between EU consumer law and other EU legislation (emerging issues and possible legal gaps).

A series of technological developments in digital markets and services were examined, and their potential impact on the ongoing fitness for purpose of EU consumer law in future has been considered. These relate to the emergence of new technologies and / or their increased take-up in the case of technologies that have existed for some time. New technologies and developments in digital markets and services raise many issues regarding consumer law, such as: how far some technologies and market changes may exacerbate digital asymmetries, how best to mitigate these, the extent to which consumer law can be complied with across different technological platforms (centralized, decentralized, distributed), the implications of an intensive and extensive use of automated systems by consumers (AI-enabled digital assistants, bots), types of smart devices and whether smart contracts in a DLT environment can be used in a way that still respect consumer law.

However, it should also be recalled that new technologies can be beneficial from a consumer protection perspective. For instance:

The **emergence of tools such as virtual/digital assistants and price comparison websites/apps can help consumers overcome or, at least, mitigate informational asymmetries.** Such tools could help to address and mitigate some of the digital asymmetries identified in this report and commented on by stakeholders such as consumer associations,

Ministries and CPAs in their responses to the targeted consultations. These assistance systems and devices can provide consumers with more information, verify data, and provide explanations or enhance the comprehensibility of the terms or the information provided by traders. Even such systems and devices may include functionalities to personalise the information that the consumer receives and must process for a specific transaction. Or simply, digital assistants and other assistance systems would significantly reduce the transaction costs that consumers bear by facilitating searches, or comparing tasks, providing ratings, or rankings, and recommending offers or traders based on (personalised) parameters. Therefore, whether traders prevent the use or limit it by consumers of such assistance systems, it might be considered that consumers' opportunities to enhance and reinforce their position is jeopardised.

The **potential use by CPAs of digital tools to strengthen the effectiveness of enforcement by automating, or at least partially automating some compliance checking tasks**. This could help to improve the number of websites and other digital platforms checked for compliance. This would be beneficial for compliant traders too. In fact, automation can improve the effectiveness of both compliance obligations and enforcement and supervision powers. For compliant traders, costly reporting obligations may be (fully or partially) automated or assisted by automated means. Traders can also deploy automated systems to pre-check themselves whether compliance seems to be complete and correct or to schedule and plan compliance milestones and prevent delays or mistakes. On the other hand, CPAs may employ automated systems and digital tools for flagging, predicting, prioritizing, compliance checking or enforcing tasks.

The **use of AI for age estimation based on user-generated content can support greater protection of children in online spaces**. The use of such technology can ensure children and young people are provided with online spaces that have age-appropriate designs. This could include the implementation of measures for children such as default private account settings, amended advertising, and preventing unwanted contact from unknown adults. A small number of EU Member States, such as the Netherlands, Ireland, and Sweden, as well as the UK and the US State of California have taken steps in this regard, including through codes of practice and guidance on age-appropriate design or the rights of children online.³¹²

Developments in new technologies, as well as the anticipated impacts on consumer protection (both positive and negative) and possible effects on the ongoing fitness for purpose of EU consumer laws are summarised below.

Concerning AI, there is an increase in the use of AI and machine learning (ML) technologies in e-commerce websites, apps and platforms that consumers use. The emergence and rapid evolution of Large Language Models (LLM) (e.g. ChatGPT) – significant stimulus to wider use by consumers. According to various market research reports, the global AI market was estimated to be between \$87-428 billion in 2022 (approx. €81-399 billion). While significant variations exist between estimates, the past and anticipated future growth trajectory is clear. One estimate suggests this has increased from around \$3 billion in 2016 (approx. €2.8 billion), while many sources anticipate continued growth (e.g. to \$1,591 – 1,847 billion by 2030 – approx. €1,485 – 1,724 billion).

The IDC notes that the AI market in the EU-27 is expected to reach €178 billion by 2026, based on a compound annual growth rate (CAGR) of 25.5% despite recent and ongoing market challenges (e.g. war in Ukraine, inflation, IT budget cuts, tech company layoffs). The characteristics of existing AI and ML systems (including mutability, opacity, need for large volumes of data, autonomy and learning capabilities) lead to general challenges related to: robustness and predictability of systems; transparency and 'explainability' of outputs; security

³¹² See, for instance: UK Information Commissioner's Office (ICO), (2023), [Age appropriate design: a code of practice for online services](#); and Yoti, (2023), [The Age Appropriate Design Code for businesses](#).

and resilience; fairness and discrimination; and privacy and data protection. While there is significant work ongoing, including in the regulatory sphere concerning the AI Act, to tackle these challenges, problems are still likely to manifest in a range of ways in the context of EU consumer law. On the other hand, AI systems have the potential to bring extensive benefits to both consumers and industry. Key considerations include:

Digital asymmetries – integration of AI technologies could exacerbate information asymmetries. In the first instance, consumers often do not know or understand that AI tools are being used by websites/apps/platforms to affect their experience or by traders they are interacting with. Second, the average consumer is unlikely to be able to comprehend how these tools are designed and developed, what inputs they use and how a particular output is determined, leading to difficulties in the consumer establishing harm or proving unfairness. Consumers may be affected by decisions that produce legal effects or otherwise significantly affect them, without being aware of the reasons, the criteria employed or the data used to generate such an output. In fact, for more complex AI systems, even the developers and engineers may be unable to fully assess the mechanisms by which an output is produced, thereby limiting its ‘explainability’ (i.e. black box models). BEUC position paper³¹³ considers AI systems to be “*instrumental in creating and perpetuating an ongoing state of asymmetry in the digital consumer-trader relationship*”. AI-driven algorithmic personalisation of interfaces and content make it more efficient for traders using AI systems to “*drive user monetisation and conversion rates. This translates into a new position of vulnerability for consumers that is both structural (structure of digital markets prevents consumers from interacting with market players on an equal footing) and architectural (due to the way interfaces are designed and operated)*”³¹⁴. A partial or full reversal of burden of proof could be considered if algorithms have caused harm due to an unfair practice due to digital asymmetries, including the complexity and opaqueness of AI algorithms in terms of design, due to poor training, on the basis of its operation or because of malfunction or unexpected learning.

Risks for consumers associated with the increased use of generative AI technologies – AI chatbots have become very widely used by consumers and traders. Whilst the technologies concerned offer many benefits for users, there are well-publicised concerns regarding the capacity of such systems to generate false and inaccurate information (‘hallucination’ risk), as well as offensive and hatred speech. For instance, a June 2023 study by the Norwegian Consumer Council³¹⁵ highlighted the risks that generative AI can result in misleading information being provided to consumers and called for increased regulatory protection. “*Generative AI models are fundamentally designed to reproduce existing material, although in potentially novel ways. This means that such models are inherently prone to reproducing existing biases and power structures*”. Generative potential of AI can also aggravate risks of deception or manipulation. From deep fakes to simply undisclosed AI-created content, consumers can be exposed to misleading content, highly-credible dis/mis-information contexts, or manipulative messages.

There is a **lack of case law presently on the risks presented by chatbots in the provision of information that could be unfair or misleading**. However, there is a 2024 tribunal case from Canada, commented on recently by EU consumer law academics as being interesting though lacking legal precedent as detailed legal argumentation was not advanced. The case involved a consumer who was provided with incorrect information by a chatbot on Air Canada’s website which contradicted information provided elsewhere on their website.³¹⁶

Overcoming information asymmetries – integration of AI technologies into personal

³¹³ BEUC (2021) Position paper - Regulating AI to protect the consumer (Frederico Oliveira da Silva and Kasper Drazewski) https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf

³¹⁴ BEUC, Regulating AI to protect the consumer. pg. 34.

³¹⁵ GHOST IN THE MACHINE - Addressing the consumer harms of generative AI, , Norwegian Consumer Council, June 2023 <https://storage02.forbrukerradet.no/media/2023/06/generative-ai-rapport-2023.pdf>

³¹⁶ Moffatt v. Air Canada, 2024 BCCRT 149 (CanLII), <<https://canlii.ca/t/k2spq>>, retrieved on 2024-02-23

assistants and chatbots can provide a means by which to provide and explain information to consumers in a more efficient and targeted manner, as stressed above. AI technologies can be both a positive tool to help consumers make informed choices, but consumers lack technical knowledge to understand algorithms and check if they have been subjected to an unfair practice or misled. Should consumers start relying on information collected, filtered, or verified by digital assistants in adopting their (informed and rational) decisions, the risk of conflict of interests emerges. The system can be designed, trained, or operate in a way that leads to self-preferencing practices, exploitative practices or other unfair results. Particularly concerning in this regard are the effects of recommender system/functionalities that may have a substantial impact on consumers' decisions with a high risk of materially distort the economic behaviour of the average consumer. Underlying these concerns is the fact that presently there is **a lack of clarity as to whether a consumer is engaging with an AI-driven chatbot or human**. One of the most visible effects of the advancement on sophisticated chatbots and personal assistants is how they have transformed human-robot interaction. Therefore, a right to access a human interlocutor on request (right to human intervention) in any circumstances is to be discussed carefully. While a right to request a human interlocutor may better protect consumers, a generalized and indiscriminate exercise of such requests may jeopardize the expected benefits of automation. Hence, views are conflicting and some consumer groups are concerned that the AI Act does not go far enough in ensuring consumer protection.

Concerning LLMs, the main developments in this context could be the integration of ChatGPT or alternative LLMs within website search or chatbot functions. While this could support the provision of information and tailored explanations (and questioning) of that information to consumers, thereby tackling information asymmetries and consumer vulnerabilities (as noted above), expert commentators also highlight a range of risks and challenges, including:³¹⁷

- Potential consumer over-reliance on the outputs of such models and thus reduced consumer agency. This could be particularly true for consumers considered to be vulnerable in the digital environment.
- Potential for inaccuracy, such as making errors, asserting incorrect information, and being gullible or biased.
- Potential for manipulation by malicious actors, such as being coaxed into creating harmful or toxic content or drafting malware. Generative AI technologies have reached the mass market, yet are not presently expressly regulated.

The risk of manipulative and misleading practices occurring through increased use of generative AI is a risk not yet mentioned in the UCPD guidance and covered through the general principles-based clauses of the UCPD only, without more specific rules that could potentially be needed in future. The NCC report gives the example of misleading search results: *“The integration of generative AI models into services such as search engines can also significantly limit consumer choice. For example, in a regular online search engine, the consumer is presented with numerous search results that they may choose between. If the search engine is replaced by a text generator that provides a single answer to any query, this potentially limits the information available. If similar models are used for online shopping, this creates new avenues for platforms to self-preference products, by ensuring that the platform’s preferred product is the only or the primarily suggested purchase”*. (pg.18).

Potential for preventing consumers from being able to verify the correctness or the provenance of the information provided by the large language model (LLM) or used by it in the generation of the output. This reduces the capacity of the consumer to use credibility indicia (a test used by courts when a hearsay statement does not fall under a specific hearsay exception) or to re-confirm the information in the original source.

³¹⁷ For instance, see: National Cyber Security Centre (2023), [ChatGPT and large language models: what's the risk?](#)

Concerning **connected products in the Internet of Things**, there has been a rapid proliferation of connected devices, driven by cloud-based infrastructure and services, edge computing capabilities and telecommunications network developments (5G / 6G). Typical European households have circa 20 connected devices with an estimated 13 billion globally in 2022. The European IoT market size was valued at \$2.19 billion in 2021 (approx. €2 billion), and is projected to reach \$12.30 billion by 2031 (approx. €11.5 billion), growing at a CAGR of 19.0% from 2022 to 2031. Digital transactions have moved beyond the conventional purchase of products, services and digital content via e-commerce websites using an order button alone. In future, there could be many transactions conducted through screenless and voice-activated devices rather than the consumer confirming the transaction through a purchase button in the final stage of a multi-click transactional process.

BEUC's 2021 position paper on the implications for protecting European consumers in a world of connected devices identifies some challenges relevant to the fitness check.³¹⁸ These pertain to data protection and privacy of IoT devices, contractual information and unfair contract terms. Examples are:

- **Data protection and privacy. Consent (Art. 7 GDPR):** According to BEUC, “the small size and lack of a physical interface on many connected devices can make it difficult for users to know how their data may be used. To comply with the GDPR and depending on the purposes for which data is processed, users will often have to be asked for consent to their personal data being collected and used, and if the service provider wishes to use this data for other purposes, users should be asked for a separate consent in a clear and explicit manner. Consent should always be informed and freely given. Service providers should not make the use of their devices contingent on the user consenting to the reuse of personal data for other purposes.
- BEUC also recommends that **legal obligations for producers and users of AI systems** should “start from the principle that some basic principles and obligations (e.g. regarding fairness and transparency) should be applicable to all AI applications”.
- Recommendations on how the CRD should optimally be applied in an IoT context were also made by BEUC. In their 2021 position paper, they noted that the CRD contains essential (pre-contractual information requirements) such that consumers can make an informed purchasing decision under Articles 5 and 6, CRD. BEUC recommended that: *“Essential information about functionality and possible limitations are clearly presented to the consumer at the point of purchase and not hidden, for instance, in the terms & conditions. For example, if the device requires an app, a stable internet connection or a subscription to function as intended, this should be made clear to the consumer prior to purchase”*.

In BEUC's view, consumers should be informed about the **business model for the device**, e.g. whether the product has been sold as a one-time payment, a subscription service or combination. Furthermore, consumers should be given information regarding the **period of time during which manufacturers will provide digital support** to the connected device.

Regarding the UCTD, challenges for consumers in deciphering whether **contract terms are unfair** due to the multiplicity of different legal documents to be consulted was cited as a problem.

- “Regarding unfair contract terms, the complexity and multi-layered nature of connected products makes it difficult for consumers to understand how exactly those products and their associated services work, and whether their rights are being respected, hampering trust in such an environment. For certain devices, consumers would have

³¹⁸ Protecting European consumers in the world of connected devices (2021) - <https://www.beuc.eu/position-papers/protecting-european-consumers-world-connected-devices>

to read many legal documents (e.g. terms of service, end-user licensing agreement, privacy statement, security policy, etc.) which are often extremely difficult to understand, leaving consumers unaware of their rights and obligations under the contract”.

- BEUC furthermore advocates that certain terms regularly used by manufacturers should be deemed unfair and blacklisted, such as when *“manufacturers reserve the right to unilaterally modify the general terms and conditions of an ongoing contract related to a connected device. This raises questions as to whether consumers have consciously consented to the new terms and whether such clauses are fair”*.

In summary, BEUC advocates updating pre-contractual information requirements and ensuring more adequate tools for consumers to express their consent at an appropriate time.

Possible legislative challenges in respect of the implications of technological developments and different means of consumers accessing essential pre-contractual information include:

Presently the CRD has an obligation to pay requirement that implies a more conventional e-commerce website setting.

Pre-contractual information requirements under the CRD are insufficiently explicit, e.g. on whether device requires “an app, a stable internet connection or a subscription to function as intended” or information at the point of sale about “how the device uses personal data” or “information regarding the period of time during which manufacturers will provide digital support to the connected device”. The period for which an IoT device will receive updates (both functional and security) is often not clear, resulting in significant numbers of consumers using devices that are no longer supported. That can lead to two possible scenarios unfavourable for the consumer. Firstly, the lack of update renders the device useless, obsolete, or defective. Secondly, the smart functionality ceases to operate due to lack of updates and that compromises the ordinary and expected use of the product embedding the smart functions. Detailed information on these aspects may condition the decision of the consumer to purchase. Likewise, these scenarios raise questions about the extent of the obligation of the trade to provide updates and the remedies available in case that the smart product turns out to be defective or underperform.

There are questions regarding the seamless provision of pre-contractual information in the IoT. For instance, a consumer orders something on their personal assistant via voice but it is not realistic for them to read on a screenless device or to listen to all the information concerned so they would be sent by email the information instead. Alternative communication means should be available in IoT devices.

The current IoT environment can engender an over-reliance on voice assistants as intermediaries between users, the devices / services they use and the providers. The power held by the provider in this interaction can therefore facilitate problematic practices in the context of EU consumer law. As above, this could be particularly true for consumers considered to be vulnerable in the digital environment. Voice messages can, on the one hand, benefit consumers in understanding and becoming aware of the conditions, but, on the other hand, they have certain limitations that may endanger its function to adequately inform the consumer (noise, language, length, degree of detail, storing and ulterior accessibility, search of specific aspect in a systematic and easy way). While voice messages can prove to be effective and appreciated by consumers for short instructions, warning, or key information, they may become inadequate and ineffective for long messages, complex terms, or complete set of pre-contractual information.

Concerning smart contracts, which use Distributed Ledger Technologies (DLT) whose execution automatically binds two or more parties based on effects they have previously defined, there is an increase of their use in certain sectors where there is scope for

disintermediation e.g. for financial transactions in cryptocurrencies, travel sector, various insurance products, renting and leasing contracts, access and use of digital content. While viable use cases and business models are still being developed and this is a nascent sector, both in terms of the technology and legal framework, the potential scale of the impact is anticipated to be significant. DG JUST has recently completed a Study on Smart Contracts³¹⁹, which builds on an earlier 2021 study on Smart contracts and the Digital Single Market.³²⁰ The study mapped the current legal framework, and reviewed how far it is possible to overcome regulatory barriers to foster wider take-up of smart contracts, whilst ensuring that EU consumer law is respected.

Previous studies note that use of smart contracts has relevance under the UCTD, CRD, UCPD and the directives on defective and non-conforming goods.³²¹ For example, the UCTD is relevant given that contract terms must be fair, clear and transparent, and unfair terms cannot be binding on the consumer. The CRD is relevant as consumers must be able to exercise their withdrawal and cancellation rights. The UCPD is relevant as smart contracts should not be concluded if the smart contract is unfair or misleading (this could be the case for instance if there is a lack of natural language explanation of coded terms). Possible legal challenges include the fact that DLT technologies used in smart contracts are meant to work on a real-time ledger and as such, contracts are not ordinarily reversible.

This makes it potentially challenging as if the ledger is meant to be time-specific and immutable, it is unclear how transactions could be reversed in some circumstances (e.g. sale of crypto assets). However, if consumer protection mechanisms (such as statutory warranties, cancellation rights) are incorporated into the design of the code for smart contracts, these could be automatically executed if built into the coding if the conditions for a reversal of a contract are triggered. Coded terms should be explained to the consumer in natural language before the contract is made. Traders should provide consumers with “*plain, intelligible summaries of smart contract code designs*” as well as “*be well advised to provide clear and informative pre-contractual literature to the consumer, explaining those terms and how they operate, in order to comply with the transparency requirement*”.³²²

Besides smart contracts, the use of automated AI-enabled systems by consumers for contractual purposes may raise uncertainties. The conditions for the validity and enforceability of contracts concluded by or with the assistance of such AI systems (digital assistants, or similar bots) used by the consumer should be clear. Otherwise, traders will be reluctant to interact with consumers assisted by digital assistants or might impede a beneficial use for consumers, and the social acceptance of such systems by consumers would be disincentivised too.

Stakeholder feedback on the impact of new technologies on relevance of EU consumer law

The stakeholder consultations investigated the degree to which the three EU consumer law Directives kept up with evolving developments in digital markets and new technologies.

Responses to the targeted survey indicated that the developments perceived to be best addressed by the Directives were the changes in digital services and markets (e.g., the increased role of marketplaces and platforms, subscription service model). More than 75% of

³¹⁹ Study on civil law rules on smart contracts, DG JUST, 2023 – study not yet published.

³²⁰ Smart contracts and the digital single market through the lens of a “law + technology” approach, DG JUST 2021. <https://op.europa.eu/en/publication-detail/-/publication/224da7da-1c18-11ec-b4fe-01aa75ed71a1/language-en>

³²¹ Forbes, Lucas, Consumer Protection in the Face of Smart Contracts (January 8, 2022). Loyola Consumer Law Review, Vol. 34, No. 1, 2022, <https://ssrn.com/abstract=4045053>

³²² Smart legal contracts - Advice to Government, The Law Commission (UK), 2021, <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf>

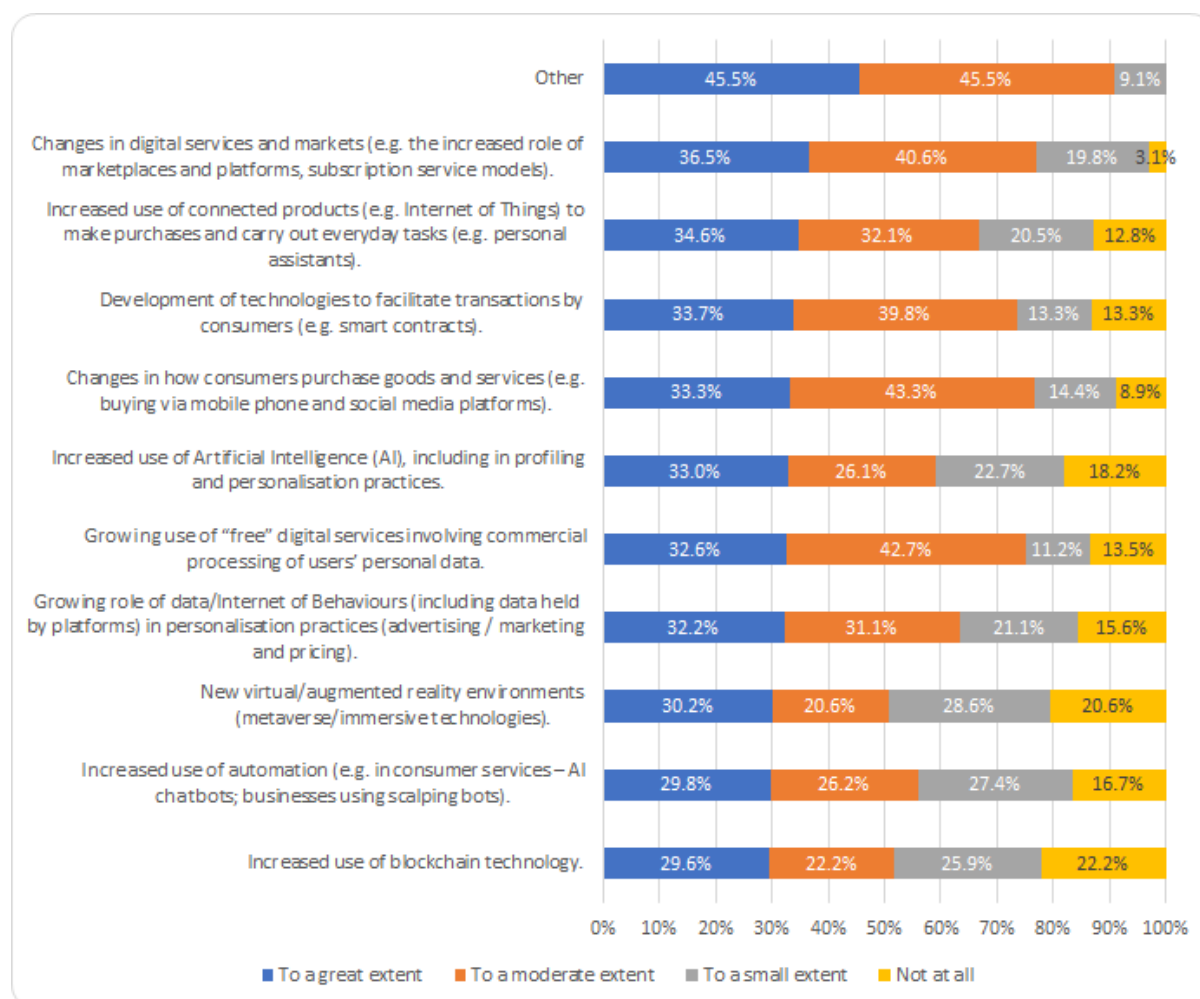
stakeholders responded 'To a great' (36.5%) or 'To a moderate' (40.6%) extent that the Directives had kept up with changes in digital services and markets.

On the other hand, the survey reported that the new developments in digital markets to which the EU Directives are less adapted are the increased use of blockchain technology, and new virtual/augmented reality environments (metaverse/immersive technologies). Among the challenges identified in wider literature on the implications for consumer law of new technologies include, inter alia: the applicable legislation in virtual worlds, privacy, identification and digital identity (avatars), whether virtual world providers are platforms or DLT models, the types of devices to access metaverse (glasses, haptics) as smart/connected products and information duties on traders relating to some of these new technologies in terms of the obligation to inform consumers about their rights, explain how privacy is protected etc. Recognising that the regulatory implications of these technologies are not sufficiently addressed presently, the Commission and the Parliament are exploring novelties and proposing an action plan.³²³

In general, the findings are mixed regarding the Directives' performance in keeping up with developments in digital markets. For all specific developments, more than 50% of respondents perceived the Directive to be relevant to at least a moderate extent; however, for some of these developments, the positive perspective only held a small majority.

³²³ <https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition> and https://www.europarl.europa.eu/doceo/document/A-9-2023-0397_EN.html

Figure 3.29 – 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)

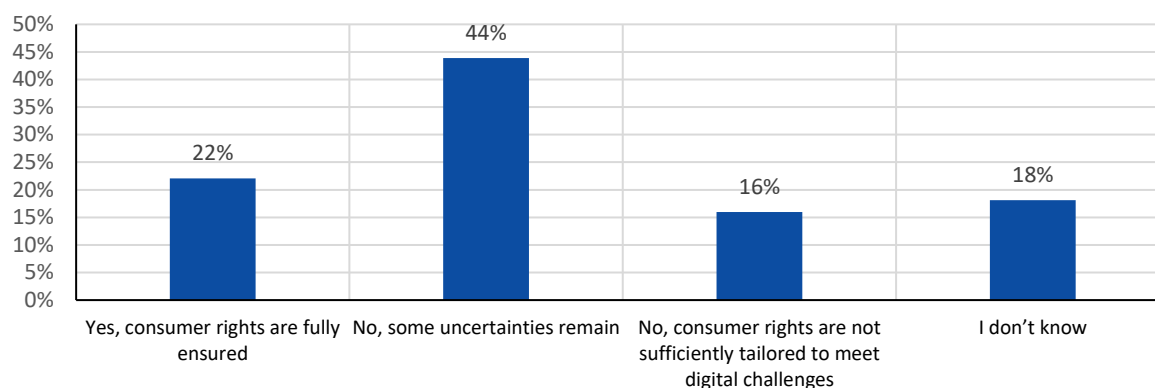


Source: targeted consultation

While the above findings reflect the feedback of stakeholders that are intimate with implementing and enforcing the Directives (or representing those that do), the findings of the consumer survey suggest that consumers have a slightly different perspective on the extent to which consumer rights have kept up with technological developments, such as the evolution of social media or the use of AI. In fact, as illustrated in the below figure, 60% of consumers (n=10000) stated that consumer rights have not kept up with such developments.

Most of these consumers indicate a more balanced view of the situation, stating that ‘some uncertainties remain’ (44%), rather than ‘consumer rights are not sufficiently tailored to meet digital challenges’ (16%). However, the findings appeared to suggest some alignment between a positive outlook on the protection of consumer rights against technological developments and low educational attainment (i.e. those that have not passed beyond ISCED 2), as well as a generally positive attitude towards spending time online. More detailed findings for both surveys can be found in Annex 6.

Figure 3.30 – Do you think your consumer rights have sufficiently kept up with technological developments, such as the evolution of social media or the use of Artificial Intelligence? (n = 10,000)



Source: consumer survey

Stakeholders across all groups commented on the impact of developments in digital markets and services, as well as the resulting developments in business models and types of traders (e.g. e-commerce websites, online platforms of various forms, online marketplaces, influencers, virtual worlds developers), on the relevance of EU consumer law.

The importance of differing perspectives and the related perceptions indicated by the above survey feedback was closely reflected in these stakeholder contributions (provided through interviews with relevant stakeholders, position papers, literature etc.).

As noted above, consumer representative stakeholders that focus on the rights and experiences of consumers, such as BEUC and the Norwegian Consumer Council, have detailed clear concerns regarding the relevance of EU consumer law in its current form to address all the risks and challenges posed by rapidly evolving digital markets.

While these stakeholders acknowledge that the general and specific objectives remain valid in this context, they highlight specific practical challenges and risks stemming from prominent developments in digital markets, including the continued prevalence of problematic practices and ensuring compliance (i.e. through sufficient monitoring and enforcement).

These concerns can stem from the nature of these emerging technologies. Considering the complex and often opaque nature of AI and machine learning systems, for instance, BEUC highlights the impact this can have on the consumer-trader relationship, placing consumers in an even weaker position characterised by greater information asymmetries.³²⁴

This was validated by academic experts in the field of digital law and new technologies, who highlighted the risk of new and emerging technologies exacerbating consumer vulnerabilities and information asymmetries, noting the fundamental challenge of the role of intermediaries in this context.

While technology can also provide solutions to these challenges, for instance by facilitating information exchange and the interrogation of information by consumers through chatbots or personal assistants), consumer associations have:

- Evidenced challenges with existing systems that can be used for this purpose. The Norwegian Consumer Council has examined the production of misleading information

³²⁴ BEUC (2021), Protecting European Consumers in the World of Connected Devices, Position Paper, Frederico Oliveira da Silva https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-091_protecting_european_consumers_in_the_world_of_connected_devices.pdf

by generative AI tools such as ChatGPT³²⁵, whilst many existing automated consumer relations systems are unsophisticated.

- Called for more systemic change that adapts the legal framework to these technologies, for instance through a partial or full reversal of the burden of proof where consumer harm has resulted from AI-driven products or services. This is highlighted as particularly important where the average consumer would be unable to establish the cause for unfair/biased outcomes or other harms, and its causation link with such caused damages. This is the solution proposed in both the revision of the Product Liability Directive, and the proposal for a Directive on AI Directive both published on 28 September 2023.³²⁶

Such stakeholders also highlight concerns stemming from business practices related to these technologies. For instance, considering connected devices and the IoT, BEUC has implied that essential information regarding the functionality and limitations of devices is not being clearly presented to consumers before purchase.

Moreover, consumer associations have highlighted concerns regarding unfair contract terms related to connected devices; for instance, manufacturers reserving the right to modify the general terms and conditions of an ongoing contract related to a connected device unilaterally.³²⁷

The consumer survey conducted for this study also illustrated the general impact of problematic practices, such as those stemming from emerging technologies. Specifically, the survey found that 27% of respondents (n = 10,000) reported financial loss or emotional distress because of relevant problems.

Industry stakeholders, on the other hand, are more reticent to change, noting that the legislation remains relevant from their perspective, considering evolutions in digital markets. They noted that more time is required to assess the extent to which the theoretical risks and challenges brought about by evolutions in technologies have any led to negative impacts in practice for consumers. Further evaluation studies are needed in their view prior to further EU legislative intervention. Additionally, these stakeholders, as well as CPAs, highlighted a range of benefits associated with new technologies, including better mechanisms for information exchange and explanation with consumers. For instance, AI-driven intermediaries, such as personal assistants or chat bots, can help consumers query terms and conditions, as well as other information on the products or services being provided.

EQ11 – How far is the digital environment sufficiently addressed in EU consumer law currently through the general principles-based approach and supporting guidance documents for each of the three Directives?

To what extent does the technology-neutral design remain relevant, or should digitalisation aspects be more explicitly regulated?

Stakeholders across the EU hold that the digital environment is generally well-served by a general principles-based approach, and that specifically the UCPD provides a balanced flexible and universal coverage for existing and emerging practices in the digital environment.

³²⁵ Ghost in the Machine - Addressing the consumer harms of generative AI, Norwegian Consumer Council, June 2023 <https://storage02.forbrukerradet.no/media/2023/06/generative-ai-rapport-2023.pdf>

³²⁶ Provisional (political) agreement has been reached on the text for the proposed revision of the EU's Product Liability Directive 85/374/EEC (PLD) and the final text of the AI Directive is expected to be published imminently.

³²⁷ BEUC (2021); and Elvy, S-A, (2016), Contracting in the age of the Internet of Things: Article 2 of the UCC and beyond, HOFSTRA Law Review, Vol. 44.839, p. 882, <https://scholarlycommons.law.hofstra.edu/hlr/vol44/iss3/10/>

However, diverging opinions between consumer organisations and traders exist as to the extent to which further and more specific regulations are required, although it is accepted that **technology-neutrality remains crucial, and that regulation requires supplementary guidance** in the form of clear examples of prohibited practices to ensure that developments in the digital environment, changes in business practices and developments in case law are reflected as soon as possible in the guidance.

Whereas traders generally preferred frequent updating of guidance over the EU taking further legislative action, consumer representatives and some Ministries more commonly expressed the view that more specific legislation could be needed to ensure ongoing relevance in some areas, even if already (implicitly) covered by the UCPD, such as dark patterns and hidden advertising.

Regarding feedback on the ongoing relevance of the legal framework in addressing the digital environment, the **general principles-based approach in EU consumer law has been underpinned by the principle of technology-neutrality**, with these general principles providing the basis for traders to assess the risk of consumer harm on a case-by-case basis. It was seen as being beneficial and increasingly relevant both for traders and consumers that an overly-prescriptive or too specific approach to regulating existing, new and emerging problematic practices should be avoided so as to preserve technology-neutrality.

Many stakeholders among traders and their representative associations perceived that the 2021 updating of the UCPD guidance by the Commission was relevant to ensure that the EU consumer law framework considers new and emerging digital practices, but without changing the general principles embedded in the EU *acquis* in this domain. Whilst the supporting interpretative UCPD guidance is not legally binding, it was seen as being **highly relevant to provide practical examples for all stakeholders as to what types of practices are prohibited**. This was seen by many interviewees and in position papers to the public consultation as being necessary as practices in the digital environment, technologies and digital markets and services evolve over time, but the legislation cannot in the view of some stakeholders (e.g. traders and their representative associations) be continually updated to reflect these developments. It can be noted that this viewpoint was shared in interviews across many industry sectors and different types of traders (e.g. e-commerce traders and marketplaces, tech / software firms, platforms).

The **technology-neutral approach was strongly supported by all stakeholders**, with limited divergence between consumer and trade representative associations. Whilst this approach was also strongly supported by national Ministries and CPAs, whilst those interviewed favoured retaining the technology-neutral approach wherever possible, they advocated that specific rules are still needed to tackle the most problematic practices, both those introduced already through the MD and possibly further rules in future, for instance, to address the lack of precision regarding the regulation of online subscriptions and also the use of certain types of personal data for personalisation practices, especially for behavioural advertising.

Consumer associations interviewed generally perceived that whilst the three core Directives have been effective overall in delivering on consumer protection objectives, **recent developments in digital markets and services and the growing size of these markets within the European and global economies means it has become necessary to introduce more specific rules to regulate problematic practices in the digital environment**. As noted earlier, BEUC and other consumer representative organisations point to an increase in digital asymmetries, as even if there is greater transparency in some areas (e.g. transactions made on online marketplaces due to the regulatory amendments stemming from the MD), consumers cannot understand the technical parameters of AI and algorithms used by traders in detail, including the weight of each criterion and the correlations between

criteria determining the output. Whilst they could be provided with more information, this would only help in providing a general understanding of decision-making criteria the AI tool is using, but not whether they were being subject to an unfair or misleading practice. However, there is today already greater transparency regarding the way in which algos work in some contexts due to EU regulatory requirements, for instance search rankings, following the Commission Notice Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council 2020/C 424/01.³²⁸

Digital asymmetries in their view represent the basis for making further changes to the EU consumer law framework to update it for the digital age. In the view of BEUC, consumer ombudsmen and some Ministries, the focus should be on further regulatory intervention in a few specific areas to address problematic practices in the digital environment where without any EU legislation, consumers would face structural disadvantages compared with traders, such as the issue of the lack of transparency and understanding of algorithms. Making such changes would in their view strengthen the relevance and maintain the effectiveness of the EU consumer law framework.

Conversely, most **trader associations and traders** expressed the view that there was **a need for more regulatory stability**, given recent changes to the legal framework. Many stakeholders highlighted the fact that as the Modernisation Directive only came into application from May 28th 2022 (and more recently than that in some Member States due to delays in transposition), they viewed it as being **too early to make further changes**, even if there are problematic practices that may not be explicitly addressed, but which are instead addressed through the guidance cited above.³²⁹ Many trader associations cautioned against regulating any further, given that the **general clauses already cover problematic practices implicitly**, an advantage of which is that there is no need to introduce new legislation each time a new problematic practice emerges as it is already covered in EU consumer law through the general clauses of the UCPD and UCTD.

This assessment was also supported by trade associations who often favoured retaining a more general principles based legal framework supported by regular updating of guidance. For instance, a trader association in the European games industry (interview, position paper with stakeholder) stated that they were in favour of improving the ongoing effectiveness and relevance of the current regulatory framework by ensuring the coherent, uniform and clear implementation of the three Directives. They **favoured the frequent updating of guidance documents to reflect new business practices and to clarify the existing legal framework's implementation** to ensure that any new problematic practices in digital markets are addressed within the guidance rather than introducing new regulatory requirements. Overall, a common theme in terms of feedback from traders and their representative associations was that there have been many changes to EU consumer law and the introduction of extensive new digital legislation recently, and cumulatively seen across the overall applicable body of EU legislation, these **changes were viewed as being too frequent**.

Stakeholders in the video games and online gaming sectors pointed out that **other EU legislation has been able to address some challenges relating to unfair personal data-driven market practices, such as the General Data Protection Regulation (GDPR) and guidance given by the European Data Protection Board (EDPB)**. The latter was seen as having been proactive in addressing this issue. Many other industry associations and individual traders also favoured retaining the current regulatory framework based on general principles rather than being too detailed in the legislation itself. **The general clauses within the UCPD already embed the principle that traders need to assess potential harm to**

³²⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC1208%2801%29>

³²⁹ Commission Notice Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council 2020/C 424/01 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC1208%2801%29>

consumers on a case-by-case basis if the commercial practice concerned could be seen as potentially unfair or misleading.

Traders in other different digital markets and services, such as tech firms managing app platforms, platforms and e-commerce traders generally favoured retaining the general principles-based approach but with frequent updating of guidance to explain how these principles could be applied in the digital environment in relation to specific technological developments, such as those highlighted in this EQ.

However, whilst wanting to maintain regulatory stability generally, some trader associations recognised nonetheless that by tackling a few specific problematic practices and legal gaps, the Modernisation Directive had brought regulatory clarity in some areas, for instance, the transparency obligations applicable to online marketplaces and their obligation to be more transparent about search rankings and identifying whether the trader is a professional or a consumer upfront in pre-contractual information.

3.3.4 Overall fitness for purpose and extent of legal gaps

EQ12 – To what extent does the legal framework remain fit for purpose to ensure digital fairness overall?

Regarding how far the legal framework remains fit for purpose, EU consumer law across the three Directives within scope was generally seen as being at least partially effective and remaining relevant in the 2017 fitness check (see EQ1) and subsequently in the present study. However, some stakeholders recognised that there are perceived legal gaps and a lack regulatory precision as to which practices are prohibited explicitly in EU consumer law due to over-reliance on the general principles based approach. These may undermine ongoing relevance from a future-proofing perspective, as evidenced by the emergence of national rules in some areas, such as for influencers and social marketing, loot boxes and cancellations of subscriptions.

To assess this question, it is first necessary to identify what is meant by the consumer law framework being 'fit for purpose' to ensure digital fairness. The assumption³³⁰ is that to remain fit for purpose in future, in the context of the digital environment, EU consumer law should:

- Continue to ensure high levels of consumer protection;
- Continue to provide a clear and stable regulatory framework that facilitates the digital single market (DSM);
- Ensure appropriate alignment with different types of EU legislation, such as to ensure that consumer protection incorporated into other pieces of law are adequately reflected in EU consumer law (such as data protection and privacy under data laws, as these are crucial to ensuring high levels of consumer protection in the digital environment);
- Safeguard fundamental rights, such as the right to privacy. There is an increasingly close connection between data protection and consumer protection, with many issues unresolved;
- Accommodate new technological developments and changes in digital markets and services (both at a systemic market level and in digital services provided by traders such as marketplaces and platforms);

³³⁰ This assumption was developed by the evaluation team and takes into consideration the general and specific objectives of the legislation, but also considers recent developments in digital markets and services, and the need for future-proofing.

- Be sufficiently adaptable to address digital commercial practices considered to be problematic and tackle these in a way that ensures ongoing fitness for purpose.

The findings from the earlier 2017 fitness check were supported in this regard. EU consumer law was found to have provided strong stability over an extended period. Stakeholders pointed to the durability of the EU consumer law framework (e.g. 30 years for the UCTD, 18 years for the UCPD and 12 years since the CRD entered into force). They also acknowledged the adaptability and flexibility inherent in the EU consumer law framework, given that national case law and CJEU rulings have helped to clarify the regulatory framework over time.

The **overarching EU legal framework (including sector-specific legislation being updated for the digital age, and digitally-focused legislation protecting consumers) was seen as evolving more rapidly** than in the past. This has implications as to whether EU consumer law may need to be updated to ensure that it remains relevant through regulatory alignment to prevent a lack of full coherence. In the interim period until the body of EU consumer law is updated, a concern among some stakeholders was (e.g. industry associations, traders) was that this could in turn lead to regulatory uncertainty for traders and consumers in future.

Some stakeholders representing traders (interviews, position papers) expressed concerns that the overall and cumulative frequency of changes to the legal framework risks continuing to increase. This was seen as being due to:

- Changes made *directly* to EU consumer law due to the Modernisation Directive (with regulatory amendments to the underlying three pieces of legislation within scope)
- Changes made *indirectly* due to consumer protection being strengthened in other pieces of EU legislation. This could result in increased regulatory uncertainty from the perspective of some traders and industry associations interviewed. In particular, the recent adoption of new legislation on digital services (through the DSA) applicable to platforms raises the issue as to whether this will require updating EU consumer law, in the future, especially the UCPD.

When considering relevance, it is also necessary to consider what might be the future potential impact on the legal framework's ongoing pertinence of moving away from a more principle-based approach towards more specific rules with greater granularity. The implications could be both positive and negative:

- For traders, there could be greater regulatory certainty regarding whether specific practices are prohibited or if they are regulated, by defining clearer rules.
- Less positively, there would be an increased volume of legislation compared with the general principles-based approach, meaning that traders would have to navigate more legislation overall. There are therefore trade-offs between avoiding over-burdening traders on the one hand, but ensuring clear rules in certain problematic practice areas on the other.
- To remain relevant, any new rules would also need to factor in the importance of future-proofing. A good example is that a cancellation button may work on an e-commerce website but is not appropriate for all design interfaces, therefore flexibility would be needed as to how rules are designed to avoid harming the competitiveness of traders.

EQ15 – How far has the Modernisation Directive (MD) ensured fitness for purpose in the underlying consumer legislation it supports (e.g. the UCPD, CRD and UCTD) through regulatory amendments?

A key issue explored through the research is the extent to which the Modernisation Directive has made a difference in strengthening the EU consumer law framework's ongoing relevance. In this regard, several findings can be noted:

- The Modernisation Directive has **helped the EU consumer law framework to remain pertinent by providing legal clarity** in respect of some digital business practices that were hitherto not specifically regulated but which were known to be problematic, such as prohibiting fake reviews, the use of scalper bots to inflate the prices of ticket sales;
- The Modernisation Directive has helped EU consumer law to remain aligned with new legislation on digital services through regulatory amendments to **strengthen transparency requirements with a focus on platforms**, a type of trader with increased economic importance but which had not previously been explicitly regulated.
- Stakeholders were generally positive about the impact of these changes on **improving the legal framework's ongoing relevance**. However, there were concerns that given that some of the changes were quite specific, this could lead to an ongoing need to regulate further specific business practices in future. An example cited in this regard was the use of scalper bots to inflate ticket prices, given that this technology could be used to increase the prices of other goods and services sold digitally.

CPAs and stakeholders tended to agree in the interviews that it is **difficult to provide an assessment** about the impact of the MD in ensuring fitness for purpose of the UCTD, UCPD and CRD by adapting them to be applied for consumer protection in digital environments. The main reason is **the recent implementation of the MD in the Member States** and the lack or very limited of case-law in this respect.

In addition, **CPAs and consumer associations** tend to converge in stressing that they expect that the MD will over time:

- **increase the level of transparency**, especially in online marketplaces, because it mandates that traders provide **essential information**, and mainly, **the main parameters determining the ranking of the offers**. This improves the ability of consumers to make informed choices.
- **enhance consumer protection when consumers provide** personal data for “free” digital services: it has filled an important gap by stating that consumers now have a 14-day withdrawal right for digital services for which they **provide personal data** but do not pay.

The analysis also confirms that, according to the CPAs and consumer associations, the most significant changes brought about by the MD concerns the introduction of **finances for breaches of the UCPD, CRD and UCTD**. It introduces stronger, **deterrent penalties** for widespread infringements affecting consumers in several Member States and deals with the unresolved issue of effectively enforcing consumer rights.

This theoretically creates a more unified approach to dealing with infringements that affect multiple states and provides a deterrent with substantial impact. However, our research shows **the gaps** and particularly that **the quantification and the practical application of these fines** varies significantly across Member States. In some states, fines may be rarely issued or kept to a minimal amount, whereas others may impose substantial fines with a focus on providing an effective deterrent. This divergence in practice undercuts the aim of the MD to harmonise fines across the EU, and potentially undermines their effectiveness as a deterrent for non-compliant businesses. If a company can expect to receive a minor fine in one state and a major fine in another for the same violation, it muddles the message of uniformity and severity that the MD seeks to enforce.

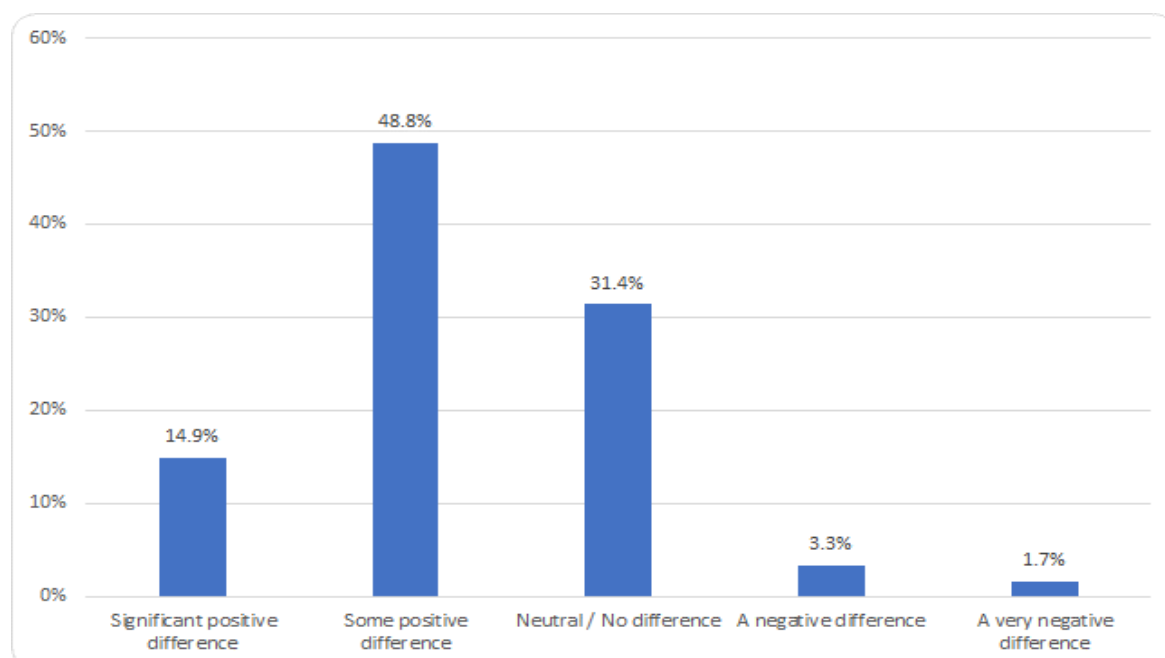
Finally, given that the regulatory amendments of the MD aimed at harmonising certain

penalties have only recently come into effect, it **may be premature to fully evaluate their impact** on actual enforcement practices across Member States. The full effects and potential adjustments may only become evident with more time and examination.

Despite the gaps above, the introduction of the MD has **undoubtedly pushed the issue of harmonisation of fines** into the spotlight in domestic jurisdictions and provided the groundwork for stronger, more uniform penalties across the EU.

As can be seen from the graph below, the Modernisation Directive’s application was perceived to strengthen the “fitness for purpose” and relevance of the underlying EU consumer law Directives concerned in addressing problematic practices. Respondents to the targeted survey were that 14.9% believed that the application of the Modernisation Directive had made a positive difference and 48.8% some positive difference. However, as high as 31.4% perceived that it had not made any difference.

Figure 3.31 – How far has the application of the Modernisation Directive strengthened the ‘fitness for purpose’ and relevance of the underlying EU consumer law Directives concerned with addressing problematic practices? (n = 121)



Source: *targeted consultation*

EQ13(1) – Can specific regulatory gaps be identified in EU consumer law due to developments in digital markets and services and due to the advent of other EU legislation, including new and existing data protection related and digital-related laws?

This EQ considers the extent to which there are perceived legal gaps in EU consumer law considering the emergence of other EU legislation. However, it is important to signpost to other parts of the report that also address legal gaps from different perspectives:

RQs 11 to 21 consider a number of specific research questions on topics that address legal gaps, for instance covering topics such as dark patterns, aggressive practices, digital addiction (including infinite scrolling and loot boxes), online subscriptions, etc.

The sections on external coherence between EU consumer law and other EU legislation consider the extent to which the adoption of new and updating of existing legislation for the digital and data ages (and across other areas of law) have left legal gaps in the EU consumer

law framework.

Legal gaps were identified, especially under the UCPD. However, as explained in the conceptual framework for the study, the nature and extent of perceived legal gaps depends not only on the current legal framework itself, but also on differences in perception between stakeholders as to what constitutes a legal gap in the first place. The general principles-based approach means that many issues relating to digital fairness and unfairness in digital markets and services and in relation to specific business practices are already covered in the existing legal framework, as made clear in the updated guidance through examples of practices that are not explicitly mentioned in the legislation but which are highlighted in guidance as examples of prohibited practices. Many business practices in the digital environment – even if they are new – are already de facto covered through the general principles-based approach in the UCPD. Therefore, the notion of legal gaps is complex and needs to be nuanced as different stakeholders may have different views as to whether these are genuinely gaps.

A key study issue is whether the absence of explicit legal rules on business practices in the digital environment means that there is a legal gap, as some stakeholders argued (e.g. in public consultation position papers, interview programme). Alternatively, is it simply that these problematic practices are already prohibited through the UCPD's general provisions, but there are low levels of awareness among traders and enforcement is weak? There is no simple answer to this question, as stakeholder views differ as to whether legal gaps exist and whether further regulatory action needs to be taken. Furthermore, there are interlinks between the positions, as the poor enforcement may be directly connected to the perception of an absence of sufficiently clear rules on those business practices.

Box 3-1 – When is a legal gap really a legal gap vs. legal clarification?

Promotional activities by influencers – legal gap, or low awareness and compliance levels about existing consumer law rules?

Several countries, e.g. FR, NL have sought to regulate influencers through new laws or guidelines (see Section 2.1.8 and case study on influencers for detailed mapping).

What's the legal position? The UCPD defines a trader but not specifically an influencer. If an influencer qualifies as a trader, they fall subject to the general provisions in the UCPD in Art's 5-9. Art. 7(2) prohibits hidden advertising and point No 22 of Annex I UCPD require that all forms of commercial communications must be clearly disclosed.

Legal gaps or regulatory clarity? Hidden ads are clearly prohibited, including on social media platforms, as made clear in the guidance. Yet there appear to be low levels of compliance by influencers. Even if the need for transparent disclosures is already clear, some stakeholders advocate the need for specific rules for influencers, as this could also bring out the distinction between promotions, sponsorship, indirect endorsements etc. rather than refer to commercial practices in a broad sense as is presently the case.

Therefore, possible future changes such as introducing a definition of an influencer and making clear specific obligations for influencers would be more about bringing legal clarity than addressing a legal gap.

Regarding enforcement, various cases have emerged in national case law, such as in Sweden and Italy that confirmed existing rules prohibiting hidden ads are applicable to influencers. Such cases have a deterrent effect, but not a sufficiently strong one, given that the CPC recently identified low levels of compliance among influencers, with only 20% of influencers clearly and consistently labelling advertising as such.³³¹ Pro-active enforcement

³³¹ Investigation of the Commission and consumer authorities finds that online influencers rarely disclose commercial content, 14th February, 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_708

by CPAs has not yet led to improved compliance levels, raising a question as to whether the existing rules are adequate.

Parallel developments to EU consumer law in other relevant EU legislation (e.g. digital laws, data laws) are also relevant to the identification of 'legal gaps'. Again, care should be taken in defining what constitutes a gap. It may be the case that new EU rules, as these have been developed in an age of digital transformation, are more explicit about particular requirements relevant to specific business practices, in a way that would not have been possible when the UCTD was drawn up (1993) and the UCPD (2005) as digital markets and services have changed beyond recognition during the interim period.

The updating of existing legislation across the EU acquis requires consideration as to whether the modernisation of other laws has implications for consumer law. Taking an example, the updating of the PLD to partially alleviate the burden of proof in the case of digital asymmetries has analogous relevance to consumer law, as consumers face persistent structural, architectural and information asymmetries for instance in choice architectures.

The adoption of new legislation in emerging areas of law, such as EU digital and data laws, may still lead to gaps as it may cover issues that are not addressed in EU consumer law, but due to the interconnected nature of laws, still require consideration as to whether updating is needed. Examples are provided of the impacts of updating existing rules and adopting new EU rules outside of consumer law on the acquis in that area under external coherence (sections 3.6-3.9).

It can be argued that whilst the general principles-based approach in EU consumer law should be retained, without more specific provisions in certain areas, this could leave legal uncertainty, as more detailed laws now exist on practices in the digital environment across other areas of EU law covering areas such as dark patterns, influencers, the use of sensitive data for personalisation practices and the protection of minors. Whilst these issues are already covered in the UCPD, there are no detailed provisions on these matters, it is rather left for the application of the unfairness test within the general principles-based provisions.

Conversely, there may be other areas where EU consumer law currently says nothing as the legislation pre-dates more recent EU legislative developments affecting digital markets and services (e.g. the use of sensitive data in personalised advertising), therefore meaning that traders rely solely on other EU legislation e.g. the DSA provisions on the use of sensitive data and Art. 9 of the GDPR, rather than on any additional legal clarity to ensure coherence in EU consumer law.

There can conversely be the reverse situation that updates to EU consumer law means a degree of inconsistency with other EU digital legislation and a consequent need for either updating or improved regulatory alignment. For example, a stakeholder in the Netherlands mentioned that whereas secondary ticketing is addressed in the Modernisation Directive, it is not applicable explicitly to platforms but rather focused on traders that resell tickets, so the stakeholder concerned suggested it should be included in the DSA.

Some stakeholders responding to the public consultation and providing position papers mentioned that this incongruence between new EU legislation and EU consumer law can cause regulatory uncertainty problems.

In the targeted survey, most respondents (56.6%), did not perceive that there are any outstanding legal gaps in the Directives. However, the targeted survey had a representation bias towards traders and their representative organisations. Moreover, 43.4% disagreed and stated that they perceived there to remain some legal gaps even if the legal framework was seen as having worked well overall.

Selected examples of EU legal gaps

Legal gaps at the thematic level were analysed under problematic practices in Section 2 and possible solutions (which includes legal gaps) are addressed in RQs 11-21. Given legal gaps are addressed elsewhere in the report, in this EQ, only summary findings are provided:

The UCPD lacks an explicit definition of dark patterns or any specific rules on the prohibition of dark patterns in online design interfaces and choice architectures.

Online subscription traps are already covered under the general clauses of the UCPD, (as made clear in the guidance) and in Annex 1, point 20 of the Directive's blacklist of unfair commercial practices. However, unlike in the rules recently introduced in certain Member States or third countries such as the UK and US (see EQ13(2) for a mapping of international rules and Section 2.1.5 for detail on subscription traps), there are no explicit rules on subscriptions. There are a few **arguable legal gaps**. Examples are:

- **Lack of any rules to make it easier for consumers to cancel subscriptions, for instance through a cancellation button.** Absence of any rules prohibiting dark patterns making it difficult for consumers to cancel such contracts as the means of cancelling may be hidden;
- **Absence of EU-wide rules pertaining to renewal reminders for online subscriptions.** Whilst many traders adopt such practices, not all do so and the case study found evidence in previous studies on subscription traps that a significant percentage of consumers have experienced difficulties in being unable to cancel such contracts.
- **Free trials** can be misleading, raising an issue as to whether these need to be further regulated, as there is no EU legislation on free trials (except insofar as these are covered by the UCPD and UCTD general clauses and in the CRD's obligation to pay (Article 8(2) Formal requirements for distance contracts).

The UCPD does not restrict the use of (sensitive) personal data from being used in personalised practices, including advertising and pricing. This is a legal gap as the interplay between the GDPR's Art. 9(1) and the UCPD is not clear for traders, creating a lack of certainty in comparison to the DSA, which prohibits the use of sensitive data for profiling purposes through targeted ads (Art. 26(3)).³³² A further gap is that the UCPD does not provide clarity as to whether psychographic profiling is legally permitted or should be prohibited in future in respect of personalised advertising.

The study supporting the 2017 fitness check recommended that the UCPD provision on vulnerable consumers should be revised and merged with the average consumer definition. This could be argued to not be a legal gap per se, but rather a possible means of strengthening the UCPD's relevance in the context of increased complexity as to what constitutes consumer vulnerability in an era of increased digital asymmetry. However, many consumer associations have argued that whilst situational vulnerability linked to digital asymmetry means that the average consumer can be vulnerable in the digital environment, this does not mean there should be less attention to vulnerable consumers.

The UCPD's Art. 5(2) provides a definition of a vulnerable consumer. However, there is an inadequate focus on protecting minors, who are at particular risk of digital addiction and have vulnerabilities due to digital asymmetries. Moreover, there is no EU-wide definition of a minor so therefore no clarity as to whether this should relate to the under 18s, under 16s etc.

Existing EU legislation fails to provide a clear definition of digital vulnerability and what

³³² Art. 26(3) - Providers of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679.

this means in practice from a legal perspective. As noted in the conceptual framework (Section 1.4), BEUC has proposed that the concept of digital asymmetry should play a role in ensuring the fitness for purpose of the EU consumer law framework to continue ensuring high levels of consumer protection in the digital environment. Many stakeholders agreed that the concept of the features of digital asymmetry are presently missing from the EU legal framework.

Targeted advertising aimed at minors is not prohibited in the UCPD but is outlawed in the DSA for platforms which is inconsistent, as such ads are banned for platforms but not for other types of traders using other digital and offline sales channels.

EQ13(2) – How far are perceived gaps being addressed by regulators in third countries?

Whilst some problematic practices are covered through the UCPD's general provisions, there is a **trend among regulators globally towards introducing more specific rules to regulate specific business practices**. The case studies identify several examples in areas such as: combatting digital addiction, preventing online subscription traps, tackling dark patterns and also protecting children from manipulative practices and digital addiction). This could be interpreted as having consequences in terms of how far the more generic principles-based approach is sufficient, as opposed to the advantages and drawbacks of having more specific rules. For instance:

- Regarding **online subscriptions (Section 2.1.5)**, in April 2023, in the UK, a standalone set of rules on online subscriptions was introduced within the **Digital Markets, Competition and Consumers (DMCC) Bill**. This imposes new duties on traders who fall within scope and provides consumers with additional protections.^{333,334}

The DMCC:

- **Right to cancel during cooling-off periods** and any renewal cooling-off periods.
 - **Requires reminder notices** - traders to proactively issue reminders to consumers before auto-renewing. Specifically, traders must give a reminder notice for the first renewal payment. For each subsequent renewal payment due six months or more after the previous payment, a cooling-off notice on the first day of the renewal period and an end of contract notice.
 - The consumer also has the **right to cancel the contract following a breach of certain DMCC rules by the trader**. Under the DMCC it is an implied term of every subscription contract that the trader will comply with its obligations to provide key and full pre-contract information, provide various notices, and facilitate termination.
- In the U.S., at federal level, on October 28, 2021, the Federal Trade Commission (FTC) published an enforcement policy statement, which warned businesses against using dark patterns to trap or trick consumers into subscription services. This aimed to eliminate **dark patterns leading to subscription traps** that the agency noted are "deceptive and unfair".³³⁵
 - In March 2023, the US FTC proposed new legal amendments regarding subscriptions³³⁶, including consideration of a cancellation button. The aim is to make it

³³³ Digital Markets, Competition and Consumers (DMCC) Bill (2023)
<https://bills.parliament.uk/publications/54208/documents/4421>

³³⁴ <https://www.penningtonslaw.com/news-publications/latest-news/2023/subscription-traps-new-law-on-the-way>

³³⁵ <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions>

³³⁶ [Federal Trade Commission Proposes Rule Provision Making it Easier for Consumers to "Click to Cancel" Recurring Subscriptions and Memberships | Federal Trade Commission \(ftc.gov\)](#)

easier for consumers to “Click to Cancel” their recurring subscriptions and memberships. There are links here with the German cancellation button.

- State laws have also been introduced setting out obligations for businesses offering **subscription-based goods and services**.
- **Loot boxes**: several countries such as Australia, China and South Korea have sought to regulate loot boxes. The UK adopted a self-regulatory voluntary initiative involving cooperation between regulators/ policy makers, the industry body and traders. Specific examples are now provided:

Regulation of loot boxes and voluntary measures by industry in third countries – selected examples:

- **Australia** - mandatory minimum age ratings, but the rules are stricter than those in say Germany.³³⁷ The USK has only been asked to consider loot box presence (without demanding a compulsory minimum age rating). In contrast, the amended Guidelines for the Classification of Computer Games 2023 of Australia (effective from 22 September 2024) require that games with loot boxes must be rated at least M (not recommended for persons under 15 years of age with no legal restrictions on access) and those with simulated gambling must be rated R18+ (restricted to adults only).
- **China**, specific rules were introduced making loot box games subject to spending limits and creating specific safeguarding measures to protect children through rules of identification, registration and payment confirmation³³⁸, which also include curfews on underage players.³³⁹
- In **South Korea**, games containing loot boxes are rated by the national regulator proactively, with discretion to refuse approval on grounds including a “game’s potential to constitute online gambling”.³⁴⁰ Rated games are then subject to parental control and supervision of children playing; South Korea also adopted rules on game spending limits for minors under the age of 19 and for adults.³⁴¹ Curfews for children in place for gaming in general, not just loot boxes.
- **UK** – self-regulatory principles were committed to by UKIE, the trade body for the UK games and interactive entertainment industry in liaison with DCMS, the responsible Ministry following extensive consultation.³⁴² Although no regulatory action was taken in relation to loot boxes, 11 principles were committed to by UKIE, the trade body for the UK games and interactive entertainment industry.³⁴³ However, a March 2024 article questioned the efficacy of self-regulation, as not all traders have adhered to these

³³⁷ In April 2021, the German Protection of Young Persons Act (JuSchG) was amended to require the German age rating organisation (the USK) to take into account the presence of ‘gambling-like mechanisms’ when making age rating decisions. This became effective from January 1, 2023. Games with loot boxes must be attached with the warning label of ‘In-Game-Käufe + zufällige Objekte [In-game purchases + random items].’

³³⁸ Xiao, L. Y. & Henderson, L. (2021) Towards an ethical game design solution to loot boxes: A commentary on King and Delfabbro. *International Journal of Mental Health and Addiction* Vol. 19, Link: <https://link.springer.com/article/10.1007/s11469-019-00164-4>

³³⁹ Xiao, L. Y. (2022) What next for video game regulation in 2022, *Computers & Law*, Vol. 144, link: <https://pure.itu.dk/en/publications/what-next-for-video-game-regulation-in-2022>

³⁴⁰ Derrington, S. et al. (2021) The case for uniform loot box regulation: A new classification typology and reform agenda, *Journal of Gambling Issues*, Vol. 46, Link: https://www.researchgate.net/publication/349350605_The_Case_for_Uniform_Loot_Box_Regulation_A_New_Classification_Typology_and_Reform_Agenda

³⁴¹ Xiao, L. Y. (2021) Conceptualising the loot box transaction as a gamble between the purchasing player and the video game company, *International Journal of Mental Health and Addiction*, Vol. 19, Link: <https://link.springer.com/article/10.1007/s11469-020-00328-7>

³⁴² [Government response to the call for evidence on loot boxes in video games - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/news/government-response-to-the-call-for-evidence-on-loot-boxes-in-video-games)

³⁴³ *Selected principles taken from industry-regulator joint guidance on loot boxes - https://ukie.org.uk/loot-boxes*

principles to date.³⁴⁴

As demonstrated in Section 2.1.8.2 which covers loot boxes and in the digital addiction case study, there have been regulatory developments both internationally and within some countries at national level within the EU-27. This raises a question as to whether there are legal gaps in EU legislation.

EQ14 – What are the possible improvements to the existing EU consumer law framework that could be considered to strengthen consumer protection?

Section 2 outlined different types of problematic practices by thematic area. It considered how pervasive these practices are and the extent to which they are already covered in EU legislation. In EQ14, we consider different ways in which improvements could be made to the existing EU consumer law framework to strengthen consumer protection. Various related research questions (RQs) were analysed as regards potential solutions to addressing specific problematic practices through *inter alia*:

- Regulatory measures e.g. consideration as to whether more specific rules might be needed in some areas, whether further regulatory clarifications and/ or updating of legislation is needed, whether the blacklists in the UCPD and / or in the UCTD need to be updated;
- Supporting soft law mechanisms e.g. how far the guidance on the three Directives which was updated in 2019 and 2021 respectively needs to be even further updated;
- How far enforcement needs to be strengthened and awareness-raised about existing EU consumer law rules in particular areas.

The research questions are summarised in Annex 1 and cover a range of topics, including whether specific rules are needed across a variety of areas, such as online subscriptions, influencer marketing, personalised advertising and pricing etc. Reference should be made to the case studies, where the problems are defined in detail, and further evidence from desk research and interviews is presented.

RQ11 – Is it necessary to reverse the burden of proof in specific circumstances of digital asymmetry between traders and consumers? (UCPD)

EQ4(1) provided an assessment of the current legal situation at EU level on issues relating to the burden of proof (BoP) in EU law. Whilst the focus was on EU consumer law, examples of a partial alleviation of the BoP to overcome digital asymmetries were provided, for instance under the PLD and the AILD in the liability law domain.

The overall findings were that there is evidence that digital asymmetries can be significant for consumers and CPAs in the digital environment given the informational imbalances between traders and consumers, which are pronounced. It was also found that some technologies, such as AI systems, including machine learning tools and the algorithms used in platforms, search engines etc. are too opaque for the average consumer, making it difficult for them to prove a particular practice was unfair, misleading or aggressive (or discriminatory in a way that makes the practice any of these).

A key tenet of EU law and national legal systems is that the plaintiff must provide sufficient evidence to avoid spurious or fraudulent legal claims being made. The possibility of a reversal of the BoP in all circumstances raises legitimate concerns from traders and trader associations that such a system could be misused. Therefore, caution should be exercised in reversing the

³⁴⁴ Video game firms found to have broken own UK industry rules on loot boxes (March 29th, 2024), the Guardian newspaper <https://www.theguardian.com/society/2024/mar/29/video-game-companies-developers-loot-boxes-regulator-complaints-rules>

BoP in EU consumer law such that this is not a blanket reversal which could risk upending the basic legal principle that the complainant (or plaintiff) must furnish satisfactory proof.

Possible solutions to address the problem are that:

As in the Product Liability Directive (PLD) and the AI Liability Directive (AILD), a partial alleviation of the burden of proof could help to strengthen consumer protection in EU consumer law, especially under the UCPD to better enable a consumer and/ or CPA acting on behalf of a consumer (or group of consumers) to investigate whether unfair, misleading and / or aggressive practices where there are digital asymmetries by placing the onus on the trader to demonstrate that particular digital services that use opaque technologies are legally compliant and not unfair.

To ensure that a balance is maintained between high levels of competition whilst not undermining business competitiveness, however, such a partial reversal of the BoP should only be in specific circumstances where there would be difficulties for an average consumer to demonstrate proof without the use of a rebuttable presumption.

Such a regulatory approach in consumer law would be analogous with that adopted in the PLD and AILD, which addresses developers of AI systems which would be too opaque for any party other than the system developer (and/ or the trader commissioning the system from a third party) to investigate.

When assessing whether there is sufficient evidence of digital asymmetry to warrant a reversal of the BoP through rebuttable presumptions, national court systems and judges should consider case law regarding what level of knowledge the average consumer might reasonably be expected to have.

It should be clarified by the Commission how far national courts can allow presumptions depending on the particular circumstances of the case, given the maximum harmonisation nature of the UCPD.

RQ12 – Is it necessary to introduce additional transparency obligations about personalised practices (taking into account existing legislation, e.g. Articles 13 and 14, GDPR)?

There are already a range of transparency obligations in relation to data gathering and processing for personalisation purposes arising from the GDPR³⁴⁵ as well as implied requirements for transparency (from the UCPD) arising from the obligation not to engage in “misleading omissions”. Further transparency measures at the point of display / contract have recently been introduced via an amendment to the CRD and the DSA. Efforts should be made in the first instance to improve implementation and enforcement of the existing measures e.g. in relation to the presentation of neutral options in the context of obtaining consent for cookies, and the consistent presentation of information around the use of automated decision-making in pricing (CRD) and the parameters used to personalise advertising (DSA).

Regarding the structure and content of the legislation, it may be relevant to consider consolidating and streamlining existing measures which relate to transparency for consumers in the digital environment to improve consistency and to facilitate enforcement. Specifically, with a view to improving transparency *at the point of display / offer / contract*, there may be scope to **require that all traders provide information about the parameters used where advertisements, offers, or prices have been adapted based on individual profiling**

³⁴⁵ GDPR requires that data subjects are given relevant information on the purposes for which personal data is processed. It also obliges data controller to inform the data subject when profiling techniques are used, and a data subject can ask the data controller about the segment in which they have been placed using profiling. In addition, Article 13(2)f GDPR requires data controllers to inform data subjects about the existence of automated decision-making (including profiling) and at least in those cases provide meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject. This information should be provided at the time when personal data are obtained.

and/or automated decision-making. Such information should preferably be presented in a standardised manner that has been tested and approved by authorities responsible for consumer protection.

Consumer associations interviewed were not in favour of removing any of the current **transparency obligations**. However, they were cautious about the possible introduction in future of any further transparency obligations in the digital environment, given concerns about the cumulative information overload in transparency requirements. Consideration should be given in future to streamlining the variety of rules e.g. transparency requirements and prohibited practices regarding profiling and personalisation to increase clarity for stakeholders and to make implementation and enforcement less complex. However, some legal academics suggested that more detailed information is needed compared with the existing provisions introduced through the MD as informing consumers that a personalisation practice has been deployed does not give them any information whether this is to their benefit or disadvantage.

Trader associations accepted existing transparency obligations as being necessary, but were not in favour of any additional rules as they viewed there as being quite significant rules on transparency through information obligations already across not only EU consumer law but also the wider body of legislation. As some of the rules were introduced recently through the MD (e.g. whether prices have been personalised, whether automated decision-making has been used in pricing), they perceived it to be soon to introduce any further obligations.

The position from the targeted consultation on additional transparency obligations about personalisation practices is shown below. There was relatively strong support for further transparency with 40.8% stating they strongly support or support further transparency, although 39.0% did not support or not support at all:

Table 3-11 – Introduce additional transparency obligations about personalised commercial practices at the moment they are deployed

Degree of support/ opposition	Number	%
Strongly support	23	23.4%
Support	17	17.4%
Neutral	10	10.2%
Don't support	29	29.6%
Don't support at all	19	19.4%
Grand Total	98	100%

- Current regulations already provide for extensive consent obligations for collecting personal data and restrict the sharing of collected data with third parties. Furthermore, existing regulations already require transparency on personalised offers and the parameters use for profiling.
- Current transparency rules could be improved to ensure that information that an offer, webpage or price is personalised and the parameters used is provided at the time when that offer, page or price is presented rather than only when the data is collected or at the time of contract but with exceptions (as is currently the case).
- From interviews and behavioural experiments, it appears that transparency obligations in the GDPR have not necessarily led to better decision-making and comprehension by consumers. Therefore, it is expected that the new obligation in the CRD to inform consumers when automated decision making is applied to pricing may similarly have a limited impact, especially as it is unclear to the consumer whether personalised pricing is to their advantage or disadvantage.

- Consumer comprehension of how personalisation is performed may become even more difficult with the increased use of algorithms and deployment of AI, given digital asymmetries, raising issues around the need for greater transparency.
- Care is needed in balancing the desire for more transparency with the risk of information overload and impacts on the user experience, where small screens or voice interfaces are used.
- To improve the ease with which consumers can exercise choice and reduce cookie fatigue, mechanisms should be introduced which allow consumers to highlight their default preferences regarding personalisation through device and/or browser settings.

RQ13 – Is it necessary to introduce a new obligation about the parameters upon which personalised commercial practice is based, in particular sensitive parameters? Is it necessary to introduce an option of non-personalisation?

The GDPR's Art. 9(1) limits the use of sensitive parameters. In addition, the DSA introduced requirements to strengthen transparency when advertising has been personalised which must be displayed and prohibited the use of sensitive parameters to target advertising on online platforms.

It may be relevant to consider generalising the obligation to reveal the parameters used for targeting, so that the obligations are not restricted to online platforms or to personalised advertising. Regarding the prohibition on the use of sensitive parameters, it may be worth considering whether prohibitions on the use of sensitive parameters for targeting should extend beyond the current provisions (which apply only to online platforms and to behavioural advertising). Specifically, the use of such parameters to tailor prices seems difficult to justify, and it is not clear why prohibitions should apply only to online platforms.

Under the DMA, gatekeeper platforms must provide an option for a less or non-personalised service.³⁴⁶ Under the DSA, very large online platforms and search engines must provide a non-personalised recommender system option. In view of the challenges that consumers face in understanding the range of available options³⁴⁷ and the preference many show for non-personalised services,³⁴⁸ it may be worth considering **extending the obligation to offer a non-personalised option (or option for tailoring based only on filters / preferences expressly selected by the end-user) beyond gatekeeper platforms (and/or introducing a corresponding right for consumers to receive a non-personalised option).**

It would be preferable for the consumer to be able to indicate their preference for a non-personalised option through a one-time amendable mechanism which could apply across all applications/websites or per application/website. From a legal perspective this could build on the mechanism envisaged in the draft e-Privacy Regulation which notes that where technically possible and feasible, consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet. For example, the Commission's "Cookie Pledge" initiative includes a discussion of the "centralisation" of consent via automated browser-based solutions or other solutions that would avoid the need to centralise

³⁴⁶ The DMA requires that gatekeepers should enable end users to freely choose to opt-in to data processing (personalisation, profiling) and sign-in practices (to multiple services of gatekeeper) by offering a less personalised but equivalent alternative unless (recital 27) a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service

³⁴⁷ A study by WIK in 2022 showed that even among 'true digital natives' in Germany there was a low level of awareness and knowledge of how algorithms work (non-existent or in best case superficial). The study concluded that does not allow consumers to make informed decisions about how to protect themselves or how they can deal with algorithmic decisions and their impact on them WIK (2022): 'Nachvollziehbarkeit und Kontrolle algorithmischer Entscheidungen und Systeme, Serpil Taş, Lukas Wiewiorra, December 2022

³⁴⁸ Although not representative, 85% of stakeholders responding to the Commission's public consultation also agreed that it would be beneficial to have the explicit option to receive non-personalised commercial offers.

choices or store them in a browser.³⁴⁹ However, some stakeholders strongly disagree with these suggestions, including many of those attending the Pledge meetings.

Regarding stakeholder feedback, there is particular concern about third parties collecting consumer data which concerns - or could be used to infer - vulnerabilities such as addictions or debt history or reveal sensitive issues regarding sexual and political preferences etc.

As regards which should be the default option in the context of a right for consumers to receive a non-personalised service (personalisation or non-personalisation), the principle that consent is needed for consumers' personal data to be used to tailor services and offers would imply that content, offers and advertisements should by default not be personalised on this basis. Consent could be given for example in the context of signing up for a service, or through settings on the device, browser or other neutral consent-management mechanism.

Regarding feedback, there was strong agreement in the targeted consultation that it should be prohibited to use consumers' data for commercial practices if it involves exploiting specific vulnerabilities for commercial purposes.

Table 3-12 – Use of consumers' data that exploits specific vulnerabilities for commercial purposes (e.g. data indicating a gambling addiction).

Degree of support/ opposition	Number	%
Strongly agree	38	45.2%
Agree	28	33.3%
Disagree	8	9.5%
Strongly disagree	10	11.9%
Grand Total	84	100%

Targeted consultation

Interviewees suggested that all profiling based on sensitive data or in relation to minors should be ex-ante prohibited.³⁵⁰ Consumer organisations favoured a **widening of ex-ante prohibitions** e.g. to include "psychographic profiling". 85% of stakeholders responding to the Commission's open public consultation also agreed that it would be beneficial to have the **explicit option to receive non-personalised commercial offers**.

An academic interviewed did not consider that personalisation should be prohibited in general but rather than ex ante prohibitions regarding the use of certain sensitive data categories could be complemented with ex-post review which could be informed through use of tools such as Computer-Assisted Personal Interviews (CAPI).

There was broad agreement in stakeholder consultations that **personalisation should not be used to exploit consumers' specific vulnerabilities, going beyond the sensitive data categories**. The UCPD could also be updated to make it clearer that sensitive data cannot be used for personalisation purposes, as in the DSA.

It may be worth considering tightening the conditions in which profiling based on sensitive parameters can be permitted i.e. reviewing the exceptions provided for in the GDPR specifically in relation to personalised offers.

RQ14 – Is it necessary to introduce new obligations and prohibitions regarding dark patterns not already expressly regulated in the UCPD or other EU laws, such as the

³⁴⁹ https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en

³⁵⁰ As noted in the previous section, certain practices are already prohibited, but prohibitions may not address all cases and personalisation can in some cases still be performed if consent is given

CRD and the DSA? Is it necessary to introduce a ‘fairness by design’/neutral interface design obligation? (UCPD)

An assessment of the problem of dark patterns was provided in Section 2.1.3. In addition, the coherence of the EU legal framework in addressing dark patterns is provided in Section 3.6 (external coherence), given that several different pieces of EU law addresses the problem, either explicitly or implicitly.

The findings from the legal mapping of dark patterns were that whilst the UCPD could capture many dark patterns, it lacks specific rules compared with other EU legislation. This can make it more difficult for CPAs to interpret and apply the rules, in comparison with the DSA, where dark patterns are **explicitly regulated under Art. 25 (1) and Art. 31**.

Whilst stakeholders agreed that UCPD guidance provides valuable examples as to which types of practices are prohibited under the UCPD’s general principles-based provisions, some stakeholders would like additional regulatory clarity either by: (1) making it explicit that dark patterns are prohibited through a dedicated provision in the UCPD, including through concrete blacklist prohibitions, and/or (2) introducing a ‘fairness by design’/neutral interface design obligation. The same recommendations were put forward by the Commission’s 2022 behavioural study on dark patterns, which entailed an in-depth evaluation of the prevalence, impacts and legal status of these practices.

Whilst the general principles-based approach has served well over the past two decades, there are concerns among consumer associations, CPAs and some Ministries that the lack of specific rules in the UCPD (except those practices included in the Annex 1 blacklist) compared with the DSA could result in a lack of coherence in the EU legal framework. Many stakeholders suggested that the interaction between the two pieces of law is unclear given the provisions in Art. 25(2) which suggest that the prohibition shall not apply to practices covered by the UCPD. This was viewed by some legal academics as risking creating regulatory uncertainty, as if for instance there is a suspected infringement by a platform, it could be difficult for a CPA to know which Directive they should pursue enforcement action under.

In addition to new prohibitions, some stakeholders, such as BEUC, some CPAs and Ministries, and some NGOs such as those working on children’s rights favoured the inclusion of a **new provision in the UCPD on ‘fairness by design’**. The purpose would be to help avoid deceptive and manipulative interface designs and functionalities from the outset, backed up by penalties as a deterrent. Fairness by design and default could for example be a useful tool to address the problem of dark patterns, which was a horizontal consideration linked to many of the problematic practices considered in detail in Section 2. This concept can be seen as analogous to the GDPR’s Art. 25 which requires data protection by default.

However, trader associations interviewed were not in favour of new requirements on dark patterns on the basis that they are already covered in the UCPD under its general principles clauses and it is made clear they are prohibited in the supporting Commission guidance. Many traders and their representative associations expressed the view that legislation should be more effectively enforced before supplementary new legal requirements are considered.

The 2023 *OECD study on dark patterns*³⁵¹ mentioned earlier states that there are different means of addressing the problem of dark patterns, ranging from (1) educational and awareness-raising among consumers and traders about dark patterns, through to (2) self-regulatory measures and (3) further regulation where necessary. The ideas presented suggest that to tackle the problem of dark patterns effectively, a holistic approach is needed. The ideas are worth highlighting below:

- Several measures to educate consumers about dark patterns, including information

³⁵¹ OECD (2022), "Dark commercial patterns", OECD Digital Economy Papers, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>.

campaigns from consumer authorities and tools to report, raise awareness about or shame businesses for dark patterns currently in use.

- Technical tools have been or are being developed to help consumers mitigate or remove dark patterns, such as browser extensions and apps and other software.
- Various self- and co-regulatory initiatives have relevance to addressing dark patterns, for example through principle-based standards governing interactions with consumers online, and some national advertising self-regulatory bodies have taken action to address various dark patterns.
- Calls among the user interface design community to raise awareness about dark patterns and adopt ethical design standards have increased in recent years, with some designers developing ethical design guidelines and toolkits.
- Mechanisms for online businesses to review their choice architecture to identify dark patterns, including self-auditing and using experiments to test compliance.

Crucially, the OECD report notes that *“whilst consumer education and technical measures and self- or co-regulatory initiatives can play an important supporting role in protecting consumers from dark patterns, they are insufficient in isolation and should be seen as complementary to robust regulatory and enforcement measures”*.

The present study confirmed the continuing prevalence of dark patterns through an assessment of relevant literature, through interviews and in position paper responses received along with public consultation responses. Regarding stakeholder feedback on potential solutions to dark patterns, feedback from the public consultation was received regarding whether stakeholders supported the introduction of fairness requirements concerning the design of online interfaces.

Table 3-13 – How strongly do you agree or disagree that: Stronger protection is needed against digital practices that unfairly influence consumer decision-making (e.g. manipulative website/app designs)?

Response options	Number	%
Strongly agree	103	46.6%
Agree	36	16.3%
Neutral	13	5.9%
Disagree	28	12.7%
Strongly disagree	33	14.9%
I don't know	8	3.6%
Grand Total	221	100.00%

Public consultation

It can be noted that addressing the problem of dark patterns horizontally could potentially solve many different business practices perceived as problematic from a consumer protection perspective. Solutions to addressing dark patterns identified through the case study research and EQs covering such practices are provided in the box below:

Box 3-2 – Solutions to addressing dark patterns

General recommendations

- Enforcement of dark patterns by CPAs should be strengthened and made more consistent. The Commission, with the support of the CPC Network and/ or consultants, could develop guidance on dark patterns. The guidance could start by clearly defining what is considered

a dark pattern, providing examples, and outlining the criteria for identifying them.

- Different sectors (e-commerce, social media, etc.) may have unique challenges. Sector-specific guidance could help target these nuances.
- Strengthen the role of national CPAs in actively monitoring for dark patterns, possibly through automated tools that can scan websites and applications.
- Create a standard checklist or framework that CPAs can use to audit websites and apps for dark patterns.
- Require CPAs to publish annual reports on enforcement actions against dark patterns, contributing to public accountability.
- Clearly outline the fines for using dark patterns, ensuring they are substantial enough to act as a deterrent.
- A public database of offenders and types of dark patterns used could be established. This could be maintained by the CPC Network or a similar entity.
- There should be clarification of the inter-relationship between the UCPD, DSA and the GDPR as concerns in which circumstances platforms should follow the DSA's Art. 25. This would improve legal certainty for traders and CPAs.

Providing real-life examples can give platforms and CPAs a better understanding of how to interpret and apply these regulations in different situations.

Protecting children and minors' rights in interface design. A preventative approach focusing on avoiding harm to children by effective design should be embedded from the outset (see position paper by the 5 rights foundation³⁵²).

Recommendations on the UCPD

- A definition should be provided in the UCPD on dark patterns. Dark patterns should be explicitly mentioned in the recitals and / or under a specific Article. The definition of dark patterns in the DSA provides a good starting point. To tackle the problem in a more effective way, an Article requiring fair/neutral design by default from the outset should be introduced. This has already been integrated into the DSA (Art. 31 (1) Compliance by design) and in an analogous way through similar rules on data privacy by design and default (Art. 25, GDPR).
- Dark patterns in website interfaces should be banned wherever the consumer is tricked into making purchases they would otherwise not have made through a transactional decision. However, given that this is a very complex area, as a consumer's perceived dark pattern might be viewed as marketing by a trader, guidance is needed to support the application, as there are likely to continue to be grey areas of delineation between acceptable and unacceptable practices.
- 'Coercion' and 'harassment' should be more clearly defined in the UCPD's Article 8 (Aggressive commercial practices) and Article 9 (Use of harassment, coercion and undue influence), in the way that it already defines 'undue influence' (Article 2). By the same token, the definition of 'undue influence' could be made to better fit the digital context.
- Annex 1 of the UCPD should be updated mentioning the specific dark patterns that should be prohibited, such as:

Misleading practices

- 1) Overly-complex contract termination interfaces requiring multiple steps to cancel a contract;
- 2) Privacy settings when traders / web designers deliberately use multiple steps

³⁵² The cost of persuasive design. <https://5rightsfoundation.com/in-action/disrupted-childhood-the-cost-of-persuasive-design-2023.html>

such that it makes it unnecessarily complicated and time-consuming to opt out of personal data sharing through choice architecture;

Aggressive commercial practice

- 3) Confirm-shaming (triggering uncomfortable emotions to influence users' decision-making). This would complement existing dark patterns in the UCPD blacklist (e.g. "bait and switch" and countdown timers).
- Introduce provisions to ensure that transactional decisions are subject to the test of interface neutrality under conditions of digital asymmetry (such that consumers do not make choices they would otherwise not have made).
 - The general principle of "fairness by design" modelled on the GDPR's Art. 25 (data privacy by design and default) should be incorporated into the UCPD. This will ensure that user interfaces and communications from traders are designed in a fair manner. Whilst dark practices are already prohibited in the UCPD, this lacks explicit clarity which such a principle would embody from the outset of the design of transactional processes.

Recommendations applicable to the CRD

- As the subscription economy is such an important sector, the principle that it should be as easy to cancel a contract as to exit from it should be established (as it is already in the guidance).
- A contract **cancellation button/functionality** should be considered at EU level, but with flexibility as to how to comply to encourage innovation in improving user-friendliness of interfaces and ease of cancellation provided traders comply with fairness by design principles. In more detail:
 - To allay concerns regarding security, any such button should not allow users to cancel contracts without logging in, a major concern of traders (both e-commerce and large platforms).
 - Evidence through interviews found that a cancellation button may work for ecommerce, but less so for other types of traders, such as platforms who have already designed user-friendly alternative interfaces to cancel contracts (e.g. through control panel settings, and settings within an app) that are regarded as less clunky and more user-centric than a cancellation button.
 - The detailed design of a cancellation button (or its equivalent) should be left to traders. However, in the CRD guidance, good practices could be highlighted e.g. avoiding too small font sizes and cancellation procedures difficult to find on a website or platform.
 - Making cancellation periods easier could be left to traders to determine whether they build in a cancellation button to their website or choose an alternative mechanism to achieve the regulatory objectives, depending on the design interface/ type of trader concerned.
 - A cancellation button should not however be overly prescriptive for several reasons: i) confining solutions to a cancellation button alone, rather than allowing different means of achieving regulatory compliance would go against technology-neutrality principles as there are alternatives means of cancelling contracts e.g. at the device level, or within app settings ii) without flexibility such a requirement would not be future-proofed to accommodate new technologies and different means of conducting transactions e.g. voice activated and iii) there are good practices in contract cancellation design on leading websites and platforms and iii) there could be additional compliance costs (website redesign).

RQ15 – Is the regulatory framework to tackle aggressive commercial practices fit for purpose? Should the current blacklist in Annex I of the UCPD on aggressive practices

be further updated to include additional digital practices?

The UCPD's scope covers protection from aggressive practices. Annex I of the UCPD gives examples of eight aggressive commercial practices prohibited in all circumstances. The following six can be applied to the digital environment:

UCPD – Annex 1 – examples of aggressive practices applicable in the digital environment.

1. Making persistent and unwanted solicitations by telephone, fax, e-mail, or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation. This is without prejudice to Article 10 of Directive 97/7/EC and Directives 95/46/EC (1) and 2002/58/EC.
2. Requiring a consumer who wishes to claim on an insurance policy to produce documents which could not reasonably be considered relevant as to whether the claim was valid, or failing systematically to respond to pertinent correspondence to dissuade a consumer from exercising his contractual rights.
3. Including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them. This provision is without prejudice to Article 16 of Directive 89/552/EEC on television broadcasting.
4. Demanding immediate or deferred payment for or the return or safekeeping of products supplied by the trader, but not solicited by the consumer except where the product is a substitute supplied in conformity with Article 7(3) of Directive 97/7/EC (inertia selling).
5. Explicitly informing a consumer that if he does not buy the product or service, the trader's job or livelihood will be in jeopardy.
6. Creating the false impression that the consumer has already won, will win, or will on doing a particular act win, a prize or other equivalent benefit, when in fact either: there is no prize or other equivalent benefit, or taking any action in relation to claiming the prize or other equivalent benefit is subject to the consumer paying money or incurring a cost.

The UCPD's Annex 1 setting out blacklisted practices currently prohibits only a few practices classified as being aggressive, but few of these are applicable to the digital environment. Unless the blacklist directly refers to specific practices, the evaluation of the aggressiveness, whether online or not, is subject to a court/authority's case-by-case assessment. It requires demonstrating that the consumer's transactional decision is (likely to be) affected. Considering the three elements that make up aggressive practices – coercion, harassment, and undue influence – enforcement investigations and activities would require behavioural insights to assess how a given practice is likely to affect consumers' actual behaviour and companies to disclose complete information about the use of behavioural experiments for the design. This lack of concrete examples of aggressive commercial practices in the digital environment, therefore, creates legal uncertainty and a risk of bearing litigation costs.

To strengthen consumer protection in combatting aggressive practices, there may be a need to update the current blacklist to tackle certain aggressive practices more specifically and ensure misleading user interfaces and data personalisation techniques do not harm consumers³⁵³. The blacklist could include personalisation practices that are considered aggressive and cover dark patterns such as confirm-shaming, which implies using language and emotion (e.g., shaming) to steer or guilt consumers into or away from making a specific

³⁵³ BEUC, "Dark patterns" and the EU consumer law acquis – Recommendations for better enforcement and reform, BEUC-X-2022-013, 07.02.2022.

choice or action³⁵⁴. The Commission's 2022 behavioural study³⁵⁵ concluded that some legislative adjustments may be necessary to better respond to dark patterns and manipulative personalisation, namely the prohibition of the most harmful practices that are not yet on the blacklist of the UCPD and the imposition of a fair/neutral design obligation on traders. The UCPD blacklist could include some established aggressive practices in the digital environment to reflect better the latter's reality, such as personalised advertising/pricing (undue influence). Potential solutions to address aggressive practices are now considered.

Box 3-3 – Possible solutions to address aggressive practices

- Coercion and harassment should be defined more clearly in the UCPD's Article 8 (Aggressive commercial practices) and Article 9 (Use of harassment, coercion and undue influence). The definitions should cover the digital context more explicitly.
- There is a need to revise the definition of 'undue influence' too, to make it more fit to the digital context – presently, it refers to the use of physical force, so it could also mention undue influence in the digital environment, with supporting examples provided in the guidance.
- In parallel, the UCPD blacklist should be updated to include further specific practices. Confirm-shaming (triggering uncomfortable emotions to influence users' decision-making) should be added to the list of aggressive commercial practices because of the influence element. Also see the solutions put forward under dark patterns for further practices that could be added to the blacklist of misleading commercial practices, but which are not aggressive.
- Identify examples of how to interpret aggressive commercial practices online through the inclusion of practical cases in the guidance.
- Create a database of aggressive practices online for CPAs and for traders to check that their business practices do not constitute bad practice.
- Support enforcement by developing guidance for, and strengthening capacity through joint work by the CPC among CPAs to identify what harassment, coercion and undue influence in different digital contexts.

RQ16(1) – Is it necessary to consider the introduction of new prohibitions or obligations to combat the problem of digital addiction, for instance in respect of infinite scrolling and loot boxes?

Section 2.1.9 of the study outlines the problem of digital addiction. This is complemented by the digital addiction case study of this report in Annex. The main findings were that digital addiction is a significant and growing problem. However, stakeholders have differing viewpoints regarding the nature and extent of the problem generally, and regarding how challenges linked to specific aspects of digital addiction, such as infinite scrolling and loot boxes, should be tackled.

The research identified evidence of the adverse impacts on the physical and mental wellbeing of consumers, and especially young people of digital addiction and/ or prolonged use of digital content and services. The European Parliament's IMCO Committee report on addictive design of online services and consumer protection in the EU single market set out extensive evidence

³⁵⁴ BEUC, "Dark patterns" and the EU consumer law acquis – Recommendations for better enforcement and reform, BEUC-X-2022-013, 07.02.2022.

³⁵⁵ European Commission, Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation – Final report, 2022.

on the potential harms of addictive design practices.³⁵⁶ This emphasised the vulnerability of minors and young adults.

Trader and consumer representatives and academic experts agreed there is a need to ensure digital fairness for consumers guided by evidence which identifies threats or ongoing harms in business practices or unwitting actions (either by individual traders or cumulatively across the digital market). As a strategic and political priority, actions which seek to address the prevalence of problematic practices and reduce consumer harm must consider also the implications that these actions may have upon both the EU digital market internally and its global competitiveness (especially for SMEs). With this understanding, this RQ considers the extent to which the efforts from platforms and traders have been sufficient in protecting consumers in respect to digital addiction, and therefore also the extent to which there is still a need to consider deeper, potentially more nuanced actions for consumer protection, and what form this may take. In parallel, the need to continue improving the coherence and enforcement of EU consumer laws, which would provide clarity and reassurance for both traders and consumers, is considered.

Infinite scrolling and other addictive design features

The research found that infinite scrolling is a problem that can exacerbate digital addiction, especially among minors. Infinite scroll arguably makes it difficult for young users to disengage as there is no natural end point for the display of new information, which constantly refreshes, which may cause them to spend more time on platforms than they anticipated and induce anxiety due to FOMO (fear of missing out), which keeps them scrolling.

In the **EU**, following the European Parliament's IMCO Committee's work on digital addiction, the EP proposed in 2023 various steps to make digital platforms less addictive, including **proposing an end to addictive design features in online services such as infinite scrolling, pull-to-refresh, push notifications and autoplay**.³⁵⁷

Social media platforms have taken some voluntary actions to limit the prevalence of infinite scrolling by interrupting the user's experience, albeit to varying degrees of intrusion. For example, TikTok introduced a feature that advises users to consider taking a break, whilst also having developed optional user self-control settings such as daily screen time management; albeit that this largely duplicates settings options already available on most devices, including Android and iOS-run mobile phones which allow for remote parental control of these settings.³⁵⁸

Regarding stakeholder feedback, from a consumer association perspective, the main concern regarding self-regulation is that infinite scroll can be addictive, especially for young people who are more vulnerable. A challenge in prohibiting infinite scrolling is that alternatives such as having a natural end point on the screen with page numbers, is regarded by platforms as an outdated design approach. Given that infinite scrolling is a standard feature of many online platforms and even many websites, there is a question as to whether regulating such design features is sufficiently technology-neutral. There are however alternative design features, such as a time out feature popping up to remind consumers how long they have spent scrolling and asking them if they wish to continue. **Loot boxes**

³⁵⁶ REPORT on addictive design of online services and consumer protection in the EU single market 8.11.2023 - (2023/2043(INI)), Committee on the Internal Market and Consumer Protection, Rapporteur: Kim Van Sparrentak - https://www.europarl.europa.eu/doceo/document/A-9-2023-0340_EN.html

³⁵⁷ <https://www.europarl.europa.eu/news/en/press-room/20231023IPR08161/new-eu-rules-needed-to-make-digital-platforms-less-addictive>

³⁵⁸ [Manage your child's screen time - Google For Families Help](#)

A summary of the nature and extent of the problem of loot boxes - and stakeholder views - was provided in Section 2.1.9 on digital addiction, specifically in Section 2.1.9.2 on loot boxes. Stakeholder views varied regarding the need to introduce new prohibitions or obligations in relation specifically to loot boxes. Stakeholders that perceived loot boxes to be encouraging gambling especially among young people were most in favour of taking regulatory action to combat the problem. The central issue with loot boxes among those stakeholders who view it as a problematic feature relates to the blurring of gambling and gaming, and the implications that this should have on subsequent transparency requirements and advertising standards of such digital products. Under this RQ, stakeholder feedback on possible solutions is provided, such as how transparency could be strengthened, whether there is a need for a prohibition, etc.

Accordingly, there is a trend towards scrutiny with regards to gambling elements in games across the US, UK, South Korea, China and most notably in the EU with the case of Belgium's 2018 restriction on loot boxes.³⁵⁹

The public consultation asked respondents whether additional transparency could be needed regarding the probability of winning in randomisation such as in video games, especially loot boxes which could help to combat the problem of digital addiction.

Table 3-14 – 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).

Response options	Number	%
Strongly agree	80	36.2%
Agree	33	14.9%
Neutral	46	20.8%
Disagree	3	1.4%
Strongly disagree	4	1.8%
I don't know	55	24.9%
Grand Total	221	100.0%

Public consultation

The results show that 51.1% either strongly agreed (36.2%) or agreed (14.9%) that there should be transparency regarding the probability of obtaining specific items. Only 3.2% disagreed, of which 1.8% disagreed strongly. It should be noted that there was a high percentage of don't knows (24.9%) among consumers. This may simply reflect the fact that not all consumers play video games and even if they do, not all would purchase loot boxes or make other in-game purchases, therefore not all respondents were familiar with in-game purchases and other forms of specific items with a randomisation element. A related question was included in respect of whether the real price in real-world currency (e.g. EUR or national currency) should be indicated for digital products priced in intermediate currency.

Table 3-15 – Require indication of the real price (e.g. EUR) of virtual items in digital products (e.g. social media, video games) when offered against intermediate currency that the user must purchase in the first step.

Response options	Number	%
Strongly support	34	44.7%
Support	13	17.1%

³⁵⁹ Xiao, L. Y. (2023). Breaking ban: Belgium's ineffective gambling law regulation of video game loot boxes. *Collabra: Psychology*, 9(1), Article 57641.

Neutral	14	18.4%
Don't support	6	7.9%
Don't support at all	9	11.8%
Grand Total	76	100.0%

Targeted consultation

The results (among those able to respond and familiar with the concept) show that 61.8% either strongly supported or supported this, a further 18.4% were neutral, whereas 7.9% did not support and 11.8% did not support at all. Not all respondents responded to this question, suggesting that whilst some consumers are familiar with the concept of virtual items, many are not.

The updated UCPD Guidance 2021 sets out the Commission's position regarding the UCPD's applicability to ensure fairness in online games, noting the presence of "gambling elements" and "addictive interface designs" in games, as well as risks to children arising from this and other known marketing practices and design strategies (No 28 of Annex I). However, most "attention-capture dark patterns" identified in the case study, such as infinite scroll, pull-to-refresh and autoplay are not explicitly mentioned in any EU legislation, even if they can be considered generally covered by the UCPD's principle-based provisions and prohibitions.

Blacklisting these types of "**attention-capture dark patterns**" through explicit inclusion in Annex I UCPD could eliminate the opportunity for users to use digital tools in a meaningful way, allow for legal challenges by the industry which is likely to adapt such features in a way that might change their classification, and disincentivise innovation in the EU market. At the same time, our case study found that through revisions to the vulnerable consumer concept in the UCPD, digital addiction could also be better addressed.

Similarly, we found that in terms of children's protection, the updated UCPD Guidance 2021 currently focuses explicitly on those practices aimed at direct exhortations of children to buy products, and video games, mobile games, or online games. Other "attention-capture dark patterns" aimed at maximising a child's time spent on a particular digital product do not receive the same level of attention.

The main justification, seen in the 2023 Video Games Europe study, against the banning of practices such as loot boxes is that a minority of users have been shown to purchase these products, whilst also there is no causal evidence at present to link this to problem gambling.³⁶⁰ Although, academic research has suggested to the contrary that these limited number of users may have significant vulnerabilities.³⁶¹ Moreover, as explored by the European Parliament's IMCO Committee's Report in 2023 and the UK Advertising Standards Agency, while loot boxes are no longer a new phenomenon, there can be adverse consequences on mental health and well-being of users, especially minors.

Their prevalence in combination also with the rise of **nuanced online marketing activities such as influencer play-along streams** (where influencers spend large sums of money far beyond that of an average consumer, let alone a child, on digital in-app content) present a significant **cumulative challenge to the online vulnerability of consumers**. In addition to this, consideration needs to be given with regard to the more direct pervasive marketing of gambling websites and betting by influencers through social media frequently viewed by children and young adults (e.g. the professional relationship on social media platforms like Instagram between betting website Stake.com and the rapper Drake).

³⁶⁰ In-Game Purchases in European Markets (2023) - IPSOS for Video Games Europe. <https://www.videogameeurope.eu/publication/in-game-purchases-in-european-markets/>

³⁶¹ Close, J. *et al.* (2021) 'Secondary analysis of loot box data: Are high-spending "whales" wealthy gamers or problem gamblers?', *Addictive Behaviors*, 117, 106851.

Moreover, the sensitivity of vulnerable consumers around peer pressure or social conformity can be compounded further by their engagement with social media, such as TikTok, YouTube shorts and Twitch streams of such games being played by others consumers.³⁶² Combined with their vulnerability as children and into early adulthood, minors and young adults often have significant time to spend, an average of over seven hours a day for 16-24 year olds, on the internet, with content and games using loot boxes or addictive features accessible from phones, tablets and gaming consoles presenting a significant cumulative exposure to problematic topics or design features.

Gambling-like features and randomised elements such as loot boxes could **contribute to addictive behaviours with implications for financial, emotional and physical wellbeing of consumers**. The most pressing issue from a consumer wellbeing perspective is the particular vulnerability and extended exposure of children and young adults to gambling as a key social element surrounding their online gameplay experience.

To protect children as vulnerable consumers, gambling elements of games whereby the user spends real or proxy virtual tokens as currency may have to be prohibited in the case of children. PEGI ratings of games should similarly reflect this in their higher designation of age-ratings (18+) for games which feature these elements in any way. Broader chance-based elements or activities within games, where in-game currencies or items are not monetisable into currencies or proxy tokens outside of the game, should be discussed further with industry stakeholders with a view to greater commitments from industry on the implementation of greater protection of all consumers from addictive design. At the same time, further future regulation, such as prohibition, should not be taken off the table – but rather addictive design elements should continue to be assessed to provide the best guiding evidence on the impacts that these may have on vulnerable consumers, in particular the cognitive development and long-term wellbeing of children and young adults.

More broadly, relating to consumers as a whole, the gamification of gambling has been seen on both ends, from game developers and gambling service providers, with the latter having an established and successful history of delivering innovative and attractive fixed-odds ‘Instant Win Games’ to consumers (online and offline) by packaging these in the form of familiar activities or board games such as wordsearches or Monopoly.³⁶³ Gambling legislation has clearly worked in a manner which has allowed traders to explore different commercial brand relationships and design models to attract consumers while also acknowledging the inherent risks of these games and the vulnerabilities facing some (if not potentially all) consumers. In this way, it is not fair upon consumers, nor upon the gambling industry, that some game developers and platforms can benefit at the expense of the consumer from insufficiently regulated features that are already well established to be potentially harmful to consumers both mentally and financially. The recommendations based on the case study on digital addiction are that:

Combatting digital addiction generally

- As digital addiction is a growing problem, especially among young people, it is necessary to proactively combat the problem. This could involve a combination of regulatory and non-regulatory measures.
- Young people have certain vulnerabilities as consumers in the digital environment (e.g. being more prone to digital addiction, less able to recognise reduced consumer choices in design interfaces and/ or to make informed choices in certain circumstances in relation to transactional decisions).

³⁶² [Guidance-on-advertising-in-game-purchases.pdf \(asa.org.uk\)](#)

³⁶³ [Confirm your purchase | Christmas Cashword | Instant Win Games | The National Lottery \(national-lottery.co.uk\)](#)

- Steps should be taken to address the problem of addictive design features on platforms, as practices such as infinite scrolling and pull-to-refresh, autoplay and push notifications, which collectively encourage addictive behaviours among users. At the minimum, there should be a requirement to give consumers the option of easily switching off these design features.
- Digital addiction is however a societal problem that cannot be solved through regulation alone. Voluntary initiatives by platforms should be encouraged in parallel to any mandatory future possible requirements.
- There should also be close partnership-working between EU regulators, CPAs and the CPC network and platforms providing digital services to experiment using a sandbox approach as to which types of technical design features are especially addictive and what types of measures are most effective in mitigating these.

Loot boxes

- New obligations could be considered to ensure transparency in respect of in-app purchases of loot boxes. Greater transparency is needed relating to the odds of receiving particular in-game benefits or items by purchasing loot boxes and, if appropriate or quantifiable³⁶⁴, the relative value of these prize items in recognised currency (such as if one were to buy the same benefit directly from the game store).
- The exposure of children and young adults to gambling-like features should be restricted.
- Transparency requirements regarding odds currently in non-binding guidance should be incorporated directly into a new provision in the UCPD to ensure transparency in fixed or variable odds.
- To address and minimise digital addiction and improve consumer awareness around the prevalence and pervasiveness of addictive practices, there must be closer alignment with tried-and-tested obligations already set out by gambling regulation.

RQ16(2) – Should the aim also be 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?

As noted in the 2023 IMCO study on digital addiction by the European Parliament, there are acknowledged as being a range of adverse consequences of digital addiction and prolonged use of digital content and services, especially on mental health. Smartphones and design features such as infinite scrolling are contributing to a rise in “behavioural patterns mirroring addiction” which can predispose any user, but especially vulnerable consumers, to develop wider mental health problems and future unhealthy relationships with gambling. These impacts are considered in further detail in Section 2.1.9.3 (the impact of digitalisation on people’s mental health).

Irrespective whether regulatory measures or voluntary measures or a combination of the two are adopted as a means of tackling the problem of digital addiction, the policy objective could indeed be to ensure higher levels of consumer protection against the negative effects on consumers of digital addiction and prolonged use of some digital content and services. This would help to reduce the adverse health, social and financial effects of these phenomena. The

³⁶⁴ Video Games Europe mentioned during interview that they supported the Commission’s efforts to strengthen transparency of the odds of winning in loot boxes. However, they did not agree that there should be regulation of virtual items and currencies always requiring real-world equivalent FIAT pricing of the purchase of virtual items. The main concern related to the risk that consumers could mistakenly think that all in-game items have a real-world value which is not the case.

focus first and foremost should be on protecting young consumers, but also the average consumer, given not only minors are subject to digital addiction. There are however limits as to how far the EU can go in reducing the problem of digital addiction in the sense that this is a societal problem and ultimately, consumers as users of digital services and content themselves must take responsibility for their own actions and choices. However, alongside a possible tightening of EU legislation to combat the problem, industry can play a positive role by developing tools that alert people to how much time and / or money they have spent on platforms across different types of digital services and content.

RQ17 – Is it necessary to introduce specific rules regarding influencer marketing and other advertising practices on social media platforms?

An explanation of the challenges linked to influencer marketing and social commerce was provided in the problematic practices section (see Section 2.1.8). In addressing this RQ, a summative reminder of the problem is provided to justify the solutions. In summary, social media platforms have become a more important sales channel with increased blurring between such platforms and online marketplaces.

It is important to have a sound legislative framework and for consumers to be aware about the risks and take steps to protect themselves when making purchases via social media platforms, especially to prevent fraud. The nature of social media platforms, where user-generated content dominates, makes it difficult to monitor and regulate commercial activities comprehensively. Unlike traditional commerce platforms where transactions and promotions are more clearly defined and easier to oversee, social commerce is embedded within a web of social interactions, making it far more difficult to distinguish between what constitutes a commercial practice and what is merely social engagement.

Moreover, social commerce **interfaces with other digital ecosystems** like online marketplaces, payment systems, and advertising networks, with their own set of regulations and jurisdictional challenges. The integrated nature of these services complicates oversight, as regulators must consider multiple legal frameworks that often have overlapping and sometimes contradictory requirements. The rapid pace of **technological innovation means that regulatory frameworks often lag technological advances and market developments/ changes in business practices**, making it difficult for laws to be adapted swiftly enough to accommodate new forms of commercial practices, platforms, or consumer behaviours that emerge in the social commerce sphere.

Social commerce falls under the existing scope of EU consumer law, including the UCPD, CRD and UCTD. With the DSA, online advertising and consumer sales through online marketplaces will become more transparent, but the law did not explicitly address specific issues regarding social commerce, such as influencer marketing, in-app browsers or buy buttons. Despite the presence of a developed EU framework, several problems have emerged. Future challenges arise with emerging trends such as the increasing use of tokens, the metaverse and the growing popularity of livestream shopping. to name a few. Taking this into account, regulatory and compliance challenges are likely to emerge in future with the most important including lacking or unclear legal definitions³⁶⁵, lack of clarity and challenges in monitoring compliance.

The research highlighted that the **EU legal framework applicable to social commerce in the EU is fragmented**. Consumer protection rules address social commerce indirectly (**UCTD, UCPD, CRD, MD**), and in the **AVMSD, DSA and GDPR**, all of which aim to ensure that consumers are treated fairly and that businesses compete on a level playing field.

³⁶⁵ Lexology, 2022. Welcome to the Metaverse: Legal Issues Marketers Need To Consider. Available at: <https://www.lexology.com/library/detail.aspx?q=75628f2a-82a8-436a-9938-037f62cb6fbc>

Another issue is the **proliferation of national legislation and diverging interpretations on influencer marketing**, which risks creating an uneven playing field across the single market. This raises issues around whether EU legislation could be needed to avoid the proliferation of national rules on this topic.

A question was included in the public consultation regarding social commerce but with a more specific angle as to whether influencers and their legal obligations should be more clearly defined. 58.4% either agreed or agreed strongly with this, 15.4% were neutral and 10.4% disagreed with a further 3.2% disagreeing strongly.

Table 3-16 – Clarifying the concept of an ‘influencer’ (e.g. social media personalities) and the obligations of traders towards consumers would be beneficial.

Response options	Number	%
Strongly agree	81	36.7%
Agree	48	21.7%
Neutral	34	15.4%
Disagree	23	10.4%
Strongly disagree	7	3.2%
I don't know	28	12.7%
Grand Total	221	100.0%

Public consultation

Recommendations to strengthen the regulatory framework for social commerce and influencers are:

- **A clear definition of influencers and their legal obligations should be provided in the UCPD and influencer marketing should be defined as a commercial activity.** The need for **minimum thresholds as to the number of followers** could be debated. The definition should also clarify what qualifies as a commercial intent and what content is a subject to disclosure requirements.³⁶⁶
- Influencers, like any other advertisers or traders, **should be prohibited from making false or misleading communications** about the products or services they promote. In the specific context of **influencer marketing**, this could potentially be an issue due to the often personal and informal nature of influencer endorsements, which may blur the line between personal opinions and promotional content.³⁶⁷
- **Introduce the concept of ‘user generated content’ (to replace ‘editorial content’) in the UCPD.** Introduction of the concept would aim to bring legal clarity and ensure that all content posted by content creators is subject to the transparency rules, regardless of whether the users promote products on a sporadic or recurrent basis.
- **Influencer agencies and brands.** EU law could be updated to ensure the influencer marketing value chain, including influencers themselves, agencies and brands is within the scope of consumer protection laws. For instance, influencer agencies and brands could be required to monitor the compliance of influencers with EU and national laws, and they could be held liable for any violations that occur.
- **Hold influencers accountable for misleading or deceptive content** that they post.

³⁶⁶ Trzaskowski, J., 2018, Identifying the Commercial Nature of ‘Influencer Marketing’ on the Internet, Scandinavian Studies in Law, 65, 81-100., Copenhagen Business School, CBS LAW Research Paper No. 19-06 at <https://ssrn.com/abstract=3324103><https://www.beuc.eu/position-papers/influence-responsibility-time-regulate-influencer-marketing>

³⁶⁷ Riefa, Christine and Clausen, Laura, Towards Fairness in Digital Influencers’ Marketing Practices (April 12, 2019). 8 (2019) Journal of European Consumer and Market Law (EuCML), Available at SSRN: <https://ssrn.com/abstract=3364251>

This could include fines or other penalties.

- **Create a self-regulatory body for influencers.** A self-regulatory body could be created to oversee the activities of influencers and to develop and enforce codes of conduct. This would help to ensure that influencers are held to high standards and that they are accountable for their actions.
- Ban the promotion of **harmful products and services.** Influencers should be prohibited from promoting products or services that are harmful to consumers, such as tobacco, alcohol, aesthetic surgeries, financial services which expose consumers to a high risk of financial loss and gambling.
- In the context of the EU, the UCPD aims to establish a harmonised set of rules across member states, the **cross-border aspect** of social commerce can still pose challenges. **An influencer based in a non-EU country** promoting products to an EU audience would technically fall under the scope of EU law when directing commercial practices toward EU consumers. Enforcing this, however, can be complex, time-consuming, and costly. **International cooperation** between regulatory bodies should be strengthened leading to more robust enforcement mechanisms. Technology itself can be leveraged to develop **automated compliance checks** and **reporting tools** to monitor cross-border activities in real-time.
- Additionally, it is important to monitor developments relating to **emerging phenomena**, that have been examined in the case-study, such as: **livestream shopping, shopping in the virtual worlds** (e.g. shopping into the metaverse), and **the trading of digital assets (e.g., fungible and non-fungible tokens)**. These emerging business practices could be covered in the Directives' guidelines.

RQ18 – Is it necessary to introduce further rules on personalised pricing and price discrimination?

Reference should be made to Section 2.1.7 Personalised pricing, which sets out the nature and extent of the problem and the degree of prevalence of personalised pricing, its impact, and how far existing EU legislation covers the topic. In addition, a case study on personalised pricing provides additional detail.

Through the MD, disclosure rules on when personalised pricing is being used at the point of sale were introduced for the first time. The case study research on the personalisation of prices found that there are potential limitations of an EU regulatory approach focused solely on ensuring transparency by informing consumers that a price has been personalised, without any information explaining to consumers *how* prices have been personalised i.e. whether price changes have been to their advantage or disadvantage.

It may be worth considering a wider application of the option for consumers to select a 'less personalised' alternative, which is currently available only in certain circumstances under the DMA (for gatekeeper platforms) and in the DSA as regards recommender systems (for very large platforms and search engines). In addition, it could be considered whether pricing personalisation which results in charging higher prices to certain consumers than would otherwise be the case in a scenario with non-personalised prices (except pricing for standard categories of consumer) should be prohibited. An alternative could be a requirement to show what the price would be in the absence of personalisation to provide "relational" information.

Various suggestions were made as regards possible regulatory solutions in BEUC's July 2023 paper on personalised pricing³⁶⁸. BEUC recommends a 'general prohibition' on personalised

³⁶⁸ BEUC (2023), Each Consumer a Separate Market? BEUC position paper on personalised pricing. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023_097_Price_personalisation.pdf

pricing practices that use personal data to adjust prices based on behavioural predictions, such as assessing individual willingness to pay, predicting customer switching likelihood, and unfairly inflating prices for undesired consumers. Furthermore, BEUC calls for clarifications to Art. 22 of the GDPR to eliminate ambiguity regarding its application to price personalisation. While acknowledging that in some good practice cases, the ban would not apply (e.g. where pricing practices are fully transparent and use limited data specific only to the nature of the product or service offered), BEUC nonetheless recognises that authorities within the CPC Network should conduct sweeping investigations to assess how traders have implemented the provisions of MD.

- Informing consumers about automated decision making regarding personalised offers is important, but should be weighed against information overload and may not lead to better decision-making by consumers. Consideration should be given to providing consumers with tools that help them understand and make choices as well as identifying more streamlined mechanisms which allow consumers to exercise their choice (and later make changes). Current regulations already provide for extensive consent obligations for collecting personal data and restrict the sharing of collected data with third parties. Furthermore, existing regulations already require transparency on personalised offers and the parameters use for profiling.
- Current rules on transparency could be improved to ensure that information that an offer, webpage or price is personalised and the parameters used is provided at the time when that offer, page or price is presented rather than only when the data is collected or at the time of contract but with exceptions (as is currently the case).
- However, based on interviews and behavioural experiments, transparency obligations in the GDPR have not led to better decision-making and comprehension by consumers. It is expected that the obligation in the CRD to inform consumers when automated decision making is applied for pricing may similarly have a limited impact. Consumer comprehension of how personalisation is performed may become even more difficult with the increased use of algorithms and deployment of AI. Care is needed in balancing the desire for more transparency with the risk of information overload and impacts on the user experience, where small screens or voice interfaces are used.
- To improve consumers' ability to make informed choices, education programmes regarding privacy protection could be considered, in particular in schools.
- It may be worth considering a wider application of the option to select a 'less personalised' alternative, which is currently available only in certain circumstances under the DMA (for gatekeeper platforms).
- The DSA currently prohibits the use of profiling based on sensitive parameters (GDPR definition) in the context of behavioural advertising. This could also be extended to cover personalised pricing.
- Certain personalisation practices such as first-degree price discrimination (achieved by inferring the consumer's willingness to pay or "dependency" on a service) are commonly viewed as unfair. Such practices would likely result in some consumers paying more for a certain product than would normally be the case. It is difficult to see how consumers would willingly consent to the use of their data in this way. It could be considered whether pricing personalisation resulting in higher prices to certain consumers than would otherwise be the case in a scenario with non-personalised prices (except for pricing for standard categories of consumer) should be prohibited. An alternative could be a requirement to show what the price would be in the absence of personalisation to provide "relational" information.

RQ19 – Should there be more specific rules on online subscriptions to prevent subscription traps, including possible rules on the termination, length and renewal of contracts in the digital environment?

Among the issues investigated were whether specific EU rules are needed to complement the UCPD's general principles to prevent subscription traps, facilitate contract cancellations for subscriptions and to address other perceived problems among consumers such as the requirement to provide payment details for free trial subscriptions.

Considering the evolving digital landscape and the growing prevalence of online subscriptions, the need for more specific rules governing such subscriptions is a pressing question. This analysis aims to present into the diverse perspectives expressed by stakeholders through position papers and interviews, while also incorporating insights gleaned from a comprehensive case study analysis of online subscriptions. By examining stakeholder feedback and drawing upon real-life examples, this exploration seeks to provide a nuanced understanding of whether additional regulations are necessary, particularly regarding termination, contract length, and renewal of contracts within the digital environment.

The growth in the subscription economy globally has led to a rapid proliferation in the number and type of subscriptions, and their value to the European Digital Single Market (DSM).

In terms of the scale of subscription traps as the most prominent challenge facing consumers in this area, it is important to consider future implications. Evidence from the OECD indicates that traders will persist in developing novel and more sophisticated methods, thereby amplifying the intricacy and complexity of subscription traps. Furthermore, the potential for these evolving approaches to exploit consumers' individual vulnerabilities is heightened by the capacity of large online companies to experiment with new techniques, including the utilization of AI and algorithmic marketing strategies. Therefore, it becomes crucial to anticipate and address these emerging challenges effectively.

Recognising the problem of subscription traps, there have been regulatory developments both in EU Member States (e.g. DE and FR) and in third countries (e.g. the UK and the U.S.) regarding the need to regulate certain problematic practices relating to online subscriptions and to make cancellation rules fit for purpose in the digital age. This demonstrates that EU regulatory action could be warranted in the European Single Digital Market context given the economic importance of subscriptions in Europe and globally, and given the risk of divergent national legislation emerging.

RQ19(1) – Renewal and transparency in relation to online subscriptions

Regarding the timing and format of renewal information provided to consumers, a few member states, such as the Czechia, Finland, France, and Portugal, apply rules selectively to certain contract types like energy, insurance, or communication services. In France and Italy, a **double-validation process is required for any tacit renewal clause, where the consumer must sign or click twice to confirm, allowing them to cancel the contract at any time.** The overall disparity between interpretations and actions at member state level across the EU for renewals, notifications and automatic cancellations by consumers remain a salient issue.

ECC-NET has asserted the **need for both a product page as well as an order confirmation page where the price is indicated and validated by the consumer.** In these pages, the main characteristics of the subscription should be covered (starting date, duration, end date, renewal and renewal period, initial price, renewed price, deadline and form to cancel). Underlining the position on online subscriptions, whether short fixed-term or indefinite rolling, they insist that enforcement is key to the effective implementation of these recommendations.

The consumer-focused stakeholders, BEUC and the Irish CPCC are similarly in favour of **obliging traders to send reminders to consumers before automatic subscription renewals occur.** It is argued that this would present an excellent example of fairness by

design, by preventing known decision-making biases (in this case, aiding consumers who may likely forget they have a subscription).

A finding from the additional research conducted through this case study is that subscription traps without adequate pre-contractual, or sometimes also contractual or post-contractual communication are not confined to free trials. Possible changes raised by consumer associations, some Ministries, and other stakeholders such as legal academics for consideration are:

- Mandating information about the total cost of the subscription – this should be clear and transparent to prevent hidden costs, part of the subscription traps problem.
- Making it mandatory to provide a subscription contract option without automatic renewal. Given that some traders take advantage of consumers that have automatic renewal set (inertia selling, difficulties in cancelling contracts, price differentials between customers on an auto-renewal and those renewing manually), this should be offered as a possibility.
- Prohibiting deceptive designs that prevent consumers from withdrawing from a contract (exercising their RoW under the CRD) or from cancelling a contract.

Two further related issues identified in our research are that: **pricing strategies by traders lack transparency**, with a risk that some consumers pay significantly more for an identical product than others, and that there is sometimes a **lack of transparency that an initial subscription price is promotional / discounted**, and that subsequently the price charged for an automatic renewal could be 200-400% higher than the promotional price.³⁶⁹ The Commission and the CPC Network have found that problems remain in respect of the hidden costs of subscriptions (e.g. when consumers are billed less upfront and then the recurring payment is much higher).³⁷⁰

Although there has been some advancement in improving the transparency of recurring payments for subscriptions, such as a recent action by the CPC Network in 2021 targeting credit card companies to enhance compliance with the Payment Services Directive and Unfair Commercial Practices Directive, there is still a notable gap when it comes to explicit rules governing online subscriptions within the CRD. While certain articles of the CRD are relevant to subscriptions, they encompass various digital contract types and do not explicitly address subscriptions. Looking ahead, there is a need to address this gap and consider the inclusion of specific rules pertaining to online subscriptions in the CRD.

RQ19(2) – Cancellation button

As identified through the stakeholder position analysis, interviews, and national level legal precedence, the issue of a contract termination button (or equivalent functionality) in line with the principle that a subscription should be as easy to exit as it is to enter remains a key consideration under scrutiny for future EU-level action. Some national legislators, like those in Germany and France, have proposed the use of a cancellation button to address challenges associated with contract cancellations. ECC-NET most prominently support the implementation of such an unambiguous German “termination/cancellation button” on websites EU wide. However, HelloFresh SE approach the issue from the perspective of the trader, believing that, like many other traders in the Commission’s Call for Evidence, the current rules in the EU provide a high level of protect across both the offline and digital environments. Citing their business model of “rolling flexible subscription contracts [...] where

³⁶⁹ CPC network action led by Danish Consumer Ombudsman, https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en

³⁷⁰ Hidden costs of subscriptions and research by CPC Network on subscription traps and scams (2020) https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en

customers [...] have the ability to amend, cancel or pause at any time”, they call for nuance in any potential alterations to the current legislation, with a differentiation between such short-term contracts and “other subscription contracts, primarily for digital assets” where they suggest deceptive practices such as subscription traps are more prominent.

The adoption of legislation in Germany and France raises a strategic question regarding the need for similar legislation at the European level, particularly through the reform of consumer law governing online subscriptions, such as the CRD. This is necessary to **prevent the emergence of divergent rules across different countries concerning the automatic renewal of online subscriptions and the ease of cancellation, which could undermine the internal market**. Concerns have been reported regarding divergences and inadequate implementation, particularly in the energy and telecoms sectors in some EU countries like Estonia and Germany. These divergences limit consumer choice from traders and increase the burden of price risk. Initial observations from the German Federal Ministry of Economic Affairs (BMWK) and the European Law Institute (ELI) regarding the implementation of a cancellation button in Germany indicate that **compliance among traders may not be a significant barrier, but clear guidance and case law rulings will be necessary to maximise the effectiveness of such legislation**. Without harmonisation at the supranational level, delays and cross-border issues are likely to escalate. Similar arguments are being made in the US, advocating for federal-level legislation to prevent substantial divergences between states in their legislative approaches.

RQ19(3) – Payment details for free trial subscriptions

The requirement of providing payment information for many free trials often discourages consumers from signing up due to concerns related to sharing credit or debit card details and the potential risk of falling into a subscription trap. To address this issue in the future, it is argued that consumers should have the option to participate in free trials without automatically being obligated to enter a paid contract without their explicit consent. This would prevent situations where consumers are unexpectedly charged for a subscription, despite not always being adequately informed during the pre-contractual stage that they will be billed unless they cancel the free trial. Even if such information is mentioned in lengthy terms and conditions, there is no guarantee that consumers will read the fine print. By requiring active consent, this problem can be mitigated, ensuring consumers have a clear understanding and actively agree to the terms before being bound by any financial obligations. The ELI (European Law Institute) position paper argues that there should be an information duty to inform about automatic renewals to overcome information asymmetries. In their view, reminders alone are not enough, as there would have to be clear rules on these for them to be effective.

From a future-oriented industry perspective, Ecommerce Europe stressed that traders should not be expected in future to provide instant confirmation of cancellation for free trials. Meanwhile, the Association of Commercial Television and Video on Demand Services in Europe strongly asserts that collecting payment details is an effective measure to prevent the misuse of free trials, including unauthorised access to content by malicious actors or bots seeking free access. They argue that altering this model would inadvertently result in heightened piracy and a reduction in the availability of free trials for consumers.

Conversely, from a consumer protection perspective, BEUC and the Irish CPCC consider that a free trial should not require any payment details from consumers; suggesting that express consent should be required when switching from a free trial to a paid service. ECC-NET explicitly calls for an outright ban on the need to provide payment information to access free trials, and observes that subscriptions entered via social media pose a particular problem for consumers, as they often fail to provide information or links to relevant webpages regarding the terms and conditions of the contract.

RQ19(4) – The withdrawal button under the CRD

The CRD has already been playing a crucial role in driving harmonisation, particularly concerning pre-contractual information and the right of withdrawal. However, there is potential for further strengthening consumer protection against subscription traps. This can be achieved through the introduction of clearer provisions regarding both consent and cancellation of contractual agreements, as exemplified by the advancements made in German law. By offering clearer options in these areas, consumers could benefit from enhanced protection against deceptive subscription practices.

During the evaluation period, the withdrawal button was introduced in the CRD through amendments by the DMFSD, and for all types of contracts, not only financial services. The new withdrawal button should therefore make it easier for the 14-day RoW to be exercised by EU consumers when concluded at a distance.

Regarding stakeholder feedback on possible solutions for **online subscriptions**, consumer associations supported the introduction of a withdrawal button as it would facilitate consumers in exercising their withdrawal rights. They also supported the inclusion of a cancellation button, beyond the 14-day right of withdrawal, to ensure that consumers are not faced with unnecessary hurdles when exercising their rights to withdrawal or contract cancellation.

The potential advantages of the recently introduced withdrawal button are similar to those that would be applicable if a cancellation button were to be required (with flexibility as to how traders make it easier to cancel a contract depending on the type of design interface – see potential solutions under relevance – RQ14 on dark patterns) by simplifying the process for consumers and ensure that consumer rights are not needlessly complicated to exercise. However, there are trader concerns regarding the possibility of overly prescriptive website design requirements either in respect of the planned withdrawal button or a potential cancellation button. For instance, Ecommerce Europe has expressed concerns that this requirement will affect SMEs disproportionately as they will have to redesign web interfaces. Balanced against these arguments, however, it should be observed that a body of literature attests to the practical problems that consumers face in exercising their right to withdrawal and the difficulties in cancelling contracts.

A major global tech firm also pointed out that they have developed options within device-level settings to cancel contracts easily and within app's, which provides an alternative to a cancellation button. It was also suggested by some large traders that it is more costly for traders when consumers exercise their RoW than cancel the contract altogether, therefore their preference was for consumers to do the latter rather than the former. This was partly due to admin costs of establishing what percentage of a service has been used during the RoW period. This appears to be problematic for digital downloads, for example.

RQ19(1-4) – Possible solutions to address problems in online subscriptions:

Regarding recommendations on online subscriptions:

Key principles in ensuring fair digital contracts

- It should be as easy to cancel as to enter a subscription contract, as already mentioned in the UCPD guidance (Art. 9d UCPD). Making this more explicit in legislative provisions would foster the digital single market and enhance digital fairness.

Possible regulatory and non-regulatory solutions to strengthen digital fairness for consumers

- There are examples of successful non-regulatory solutions. For instance, engagement by the CPC Network with global credit card companies has led to greater transparency for consumers with online subscriptions regarding reminders ahead of the transaction, the total amount due, and contract duration. However, whilst credit card providers and traders already provide such information to consumers, not all do so.

- To ensure uniform levels of consumer protection, automatic reminders informing consumers about the date of an automatic renewal and the total payment should be automatically sent to avoid consumers paying for services they no longer require. Renewal reminders should be sent with appropriate frequency depending on the payment schedule (e.g. annual, monthly) by email and/or text.
- In the digital age, there is no reason why a consumer should be allowed to enter into a contract online but not to be able to cancel one. This could be explicitly written into EU consumer law, rather than left to guidance. The DSA's Article 25(3)(c)) shows it is possible to have explicit rules on online subscriptions to ensure it is not more difficult to enter into, than to exit from a contract.
- Whereas many free trials require payment information, this may deter consumers from signing up, given concerns in handing over credit or debit card details and regarding the potential to be caught in a subscription trap. Consumers could be allowed to participate in free trials without being automatically bound to enter into a paid-for contract without their active consent.
- This would avoid the current situation whereby many consumers end up being charged for a subscription despite not always being made aware through pre-contractual information that they are going to be billed unless they cancel the free trial. Even if they are informed about lengthy terms and conditions, there are no guarantees they will read the small-print. **Requiring active consent would alleviate this problem.**
- There should be greater transparency in informing consumers about subscriptions and their associated costs, from pre-contractual through to the contractual stages and ahead of renewals. This information could be provided automatically and would avoid consumers being ripped off without them being aware of what subscriptions they have running and the associated costs. Several measures could be taken:
 - **Automatic renewals** – at least for annual and quarterly subscriptions (monthly was seen as too frequent by some stakeholders).
 - **Mandating information about the total cost of the subscription** – this should be clear and transparent as it would help to prevent hidden costs, part of the subscription traps problem.
 - **Mandatory to provide subscription contract option without automatic renewal.** Given that some traders take advantage of consumers that have automatic renewal set (inertia selling, difficulties in cancelling contracts, price differentials between customers on an auto-renewal and those renewing manually), this should be offered as a possibility.
 - **It should be made easier for consumers to cancel contracts.** A provision could mandate the use of either a cancellation button on websites or if another type of design interface, then an alternative simple means of cancellation. A button could also be mandated. However, consideration as to the impact on SMEs of these measures should be given. There is a need to avoid an overly-prescriptive design approach, so long as cancellation and withdrawal possibilities are sufficiently accessible by website users.
 - **Preventing deceptive designs to prevent consumers from withdrawing from contracts** (exercising their RoW under the CRD) or from cancelling a contract.
- As per BEUC's 2022 recommendations for regulatory interventions on the UCPD and CRD, there is a need to tighten the definition of illegal practices to minimise or remove

entirely the opportunity for both deceptive and unclear renewal practices. There is a link with the horizontal issue of dark patterns in website design.

- A general principle of “fairness by design” should be mentioned in the recitals of the UCPD to ensure that traders consider and build-in digital fairness for consumers from the outset of the design process. This would improve transparency and fairness of digital subscriptions, ensure technical capabilities such as auto-reminders of automatic renewals are sent out.

RQ20 – Is it necessary to introduce new prohibitions or obligations regarding scalping practices?

Scalping is the process of buying products with the aim of reselling these for a higher price. People practicing scalping are called scalpers, and they typically operate in situations where demand exceeds supply — such as ticket sales (already prohibited), limited-edition product drops and online retail sales.

There are different types of bots that may engage in practices that could be unfair. The way in which these bots operate is explained below:

Scraping bots monitor web pages and scan websites for information. If a scalper wants to get their hands on a product that is out of stock, for example, they will set up a scraping bot to constantly check the product page for a restock.

Footprinting bots are like scraping bots, but instead of searching public web pages, search for hidden pages. If a scalper knows a company is about to release a high-demand item, footprinting bots may be used to test thousands of URLs to try and identify the unpublished product page.

Source – adapted from typology of different types of bots: <https://queue-it.com/blog/scalping-bots/>

The **resale of event tickets via bots** was prohibited through the MD as an unfair commercial practice under the UCPD (see Annex 1 blacklist, point 23a, as amended). This addressed a problem which some Member States were concerned about, as some of them had introduced national legislation to address the problem. However, there is a question as to whether it would be more effective to prohibit the use of bots for other types of scalping practices beyond event tickets that could lead to higher costs for consumers. Examples are:

- Scanning e-commerce sites to purchase retail goods in strong demand in advance of other consumers using automated technologies to artificially inflate costs;³⁷¹
- Buying up the supply of heavily discounted goods ahead of other consumers to access the best deals.^{372,373}
- Scanning travel portals to get the best deals ahead of other consumers.

Example in games consoles industry of scalping practices – in 2017, Nintendo’s reissue of the SNES console was a target for online resellers looking to profit from excess demand over supply. Since the product launch was announced, scalpers used bot technology to place pre-orders and promptly advertised these at two or three times the price on auction sites. This even prompted a warning from the manufacturers themselves not to

³⁷¹ <https://www.gamesradar.com/20-million-ps5-scalping-attempts-were-blocked-by-walmart-in-just-30-minutes/>

³⁷² Black Friday blighted by bots buying all the bargains

<https://internetretailing.net/black-friday-blighted-by-bots-buying-all-the-bargains/>

³⁷³ <https://www.clickz.com/why-retail-scalping-is-still-big-business-and-what-to-do-about-it/112079/>

purchase from scalpers at inflated prices.³⁷⁴

Examples of the consequences of scalping practices beyond event ticket sales are that prices become inflated, and secondly it may become difficult for shoppers to simply acquire what they want.

However, striking a balance between protecting consumers and allowing legitimate resale activities can be complex. Moreover, the effectiveness of enforcement actions can face practical difficulties due to the cross-border nature of scalping activities. Regarding potential solutions:

The use of scraping bots and footprinting bots could be prohibited in Annex I of the UCPD in any circumstances where the use of such technologies leads to consumer detriment, such as higher prices for some consumers over others, queue jumping.

CPAs through the CPC Network could also **engage with leading traders and / or their representative associations to take active measures to combat the problem** on platforms and marketplaces.

For instance, as good practice examples by traders:

- **Manual delisting of scalped items** – eBay has taken steps to delist scalped games consoles that were in short supply and purchased by scalpers. The aim was to ensure that such items were not viewable to shoppers. This requires investment by administrative staff to hunt down scalped items and to block those individual traders.
- **Scalping can also be combatted using automated digital tools**, such as through using big data to detect and prevent scalping activity and by using tests to check that consumers are human rather than a scalping bot (e.g. Amazon has used such techniques).

RQ21 – What changes are necessary to adapt or complement the existing provisions of the UCTD to better address digital challenges?

The UCTD was widely seen as being **applicable to standard contract terms in both the offline and online environment**. However, applying the provisions poses specific challenges in the digital environment.³⁷⁵ For instance, there are transparency and fairness requirements in the UCTD and their interaction is arguably more complex in the digital environment, given that digital fairness is impacted by design choice architectures³⁷⁶ and by the fact that digital vulnerability is more complex in the digital environment, as it is architectural, relational, and data-driven.

The UCTD's Article 5 provides that all contract terms must be drafted in **plain, intelligible, and unambiguous language**. The UCTD Guidance explains that this means that the terms must be clear and transparent both in substance and format. Article 3(1) of the UCTD states that the terms should not cause significant imbalances between the parties' rights and obligations to the detriment of consumers, contrary to the requirement of good faith. Otherwise contract terms are unfair and non-binding on the consumer, and can also lead to the nullity of the whole contract if it cannot subsist without the unfair terms. The Annex to the Directive lists categories of terms which could meet these criteria. The UCTD's provisions - including the examples in the Annex - are based on principles and focus on the effects on consumers arising from contractual conditions.

³⁷⁴ See <https://www.digitaltrends.com/gaming/nintendo-snes-classic-edition-scalper-warning/> and <https://www.clickz.com/why-retail-scalping-is-still-big-business-and-what-to-do-about-it/112079/>

³⁷⁵ Helberger, N. (2016). Profiling and targeting consumers in the internet of things – A new challenge for consumer law. In R. Schulze & D. Staudenmayer (Eds.), Digital revolution: Challenges for contract law in practice (pp. 135–162). Nomos.

³⁷⁶ Natali Helberger and others, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022), Journal of Consumer Policy.

There are specific issues relating to the UCTD's application in the digital environment. For instance, the growing role of data in the European digital economy means the need for **parallel application of the UCPD, the UCTD and the GDPR**, for instance regarding data exploitation strategies.³⁷⁷ The UCTD should however in principle be sufficiently flexible to handle imbalances resulting from the use of data-driven personalisation practices.

In the digital context, the UCPD's fairness test also needs to be applied in parallel with the UCTD's fairness test of standard contract terms, as there is a close interaction between the two Directives. For example, the terms of service of an online platform may include unfair commercial practices but also constitute unfair contract terms. Very lengthy standard contract terms for instance may breach the plain, intelligible, and unambiguous language requirement. In the view of stakeholders such as BEUC, there are examples of social media platforms where several contract terms were perceived to be unclear, ambiguous and/or create an unbalanced relationship between the platform and its users in favour of the platform.³⁷⁸

A further issue in the digital environment is that standard contract terms need to be adapted to the different types of users, which vary depending on the type of digital services and content. Formats should be adapted to fit their audience. As an example, social media platforms need to ensure that their terms of services are easy to understand for specific groups of users, such as children and teenagers.

A possible legal gap is that whereas the concept of an average consumer and a vulnerable consumer is embedded within the UCPD, when applying the UCTD, only a consumer is referred to. *"The necessary connection between the average consumer and transparency comes almost without saying in both the CJEU case law, and in the scholarship provisions on the UCTD. However, Articles 4(2) and 5 of the UCTD merely refer to a consumer. The focus on the average consumer therefore reduces the scope of application suggested by the plain meaning of these provisions"*.³⁷⁹

Compared with the UCPD, making changes to update the UCTD for the digital age is overall more challenging and complex for various reasons. The general principles underlying standard contract terms have been determined at EU level, however, contract law remains divergent at national level. Moreover, there is no single agreed set of fair and unfair standard contract terms as such terms vary by sector and depend on what they are about.

Some stakeholders also highlighted the need for stronger links between provisions in the UCTD and the DSA related to terms and conditions (Art. 14 which is concerned with information requirements).

Potential measures broadly related to contract terms, potentially beyond the scope of the UCTD, could include:

- Adding the most common unfair standard contract terms prevalent in the digital environment to a **UCTD blacklist** which allows Member States to complement it at national level with their own additional blacklist items.
- Further **elaborating the UCTD guidance document** to reflect specific issues which may arise from the use of data-driven personalisation insofar as they are relevant to the assessment of the fairness and transparency of contract terms.
- Ensuring that a **definition of an average consumer is included within the UCTD**.

³⁷⁷ BEUC, EU CONSUMER PROTECTION 2.0. Structural asymmetries in digital consumer markets, (2021), N. Helberger, O. Lynskey, H.-W. Micklitz, P. Rott, M. Sax, J. Strycharz, https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2_0.pdf

³⁷⁸ BEUC (2021), TikTok without filters (see chapter on unfair Terms of Service) https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-012_tiktok_without_filters.pdf

³⁷⁹ The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration European Review of Contract Law (ERCL), Vol. 18, No. 1, pp. 1-31, April 2022, DOI: 10.1515/ercl-2022-2035, Max Planck Private Law Research Paper No. 22/11

³⁸⁰ Also assess the merits and drawbacks of including a definition of a vulnerable consumer, involving legal academics, consumer and business associations. These concepts are important in the UCPD and their absence in the UCTD could be considered as undermining consumer protection. Taking the example of users of digital services who are children and minors, they arguably warrant greater attention than the average consumer to ensure that standard contract terms are clear and intelligible.

- **Improving transparency regarding the jurisdiction of standard contract terms.** Obligations should be introduced for large international traders to clearly indicate the location and jurisdiction for terms and conditions online in case of complaints, centralizing them in a single document, and ensuring easy accessibility to older versions of T&Cs. This would make sense given that there is divergence in national contract law so it is important that the consumer receives transparent pre-contractual information in this regard.
- Promoting greater awareness among traders about good practice measures to improve the understandability and clarity of standard contract terms, such as to make these more “plain, intelligible and unambiguous”. Examples of possibilities are:
 - **Prioritise the presentation of essential key information in contract terms.**
 - **A summary of the key standard contractual terms should be complemented by a link to the full contract terms.**
 - Use **visual cues and graphics** to contribute to fair digital design.
- Creating EU templates with **standard contract terms to promote consistency** where feasible.

The development of **EU-level standards and guidance** could be considered considering lessons learned from the **GDPR’s application** and its connections to privacy contract terms, as well as the emergence of new legislation aimed at regulating the digital sphere.

RQ22 – Given the UCTD’s minimum harmonisation nature, to what extent should Member States be able to regulate consumer contract terms and/ or develop national blacklists?

As a minimum harmonisation Directive, Member States are required to transpose the UCTD at national level and to meet the minimum harmonisation requirements, but retain regulatory discretion as to how precisely they should implement certain aspects of the Directive.

Member States may already implement at national level more stringent provisions in the area covered by the Directive, to maximise consumer protection. For instance, Member States may develop their own national blacklists of unfair contract terms.

Some national Ministries were in favour of retaining the ability to develop national blacklists of unfair contract terms specific to their jurisdiction.

An interviewee from the Ministry of Social Affairs and Social Protection in Austria mentioned that their national blacklist of unfair standard contract terms has been developed over 30 years and has been informed by and updated according to the rich body of national case law. Their preference was therefore for Member States to retain competence for the development of national blacklists, which was seen as having strengthened the Directive’s effectiveness and as having delivered regulatory stability over an extended period. The Ministry had a clear

³⁸⁰ The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration European Review of Contract Law (ERCL), Vol. 18, No. 1, pp. 1-31, April 2022, Max Planck Private Law Research Paper No. 22/11

position in this regard in their responses to the call for evidence and the public consultation, which was not to re-open or amend the UCTD at all.

Other stakeholders interviewed, especially among ministries, also considered the UCTD to provide the right balance between ensuring sufficient stability whilst retaining the flexibility to update the national blacklist with any new unfair standard contract terms. It was noted that Member States' ministries responsible for maintaining a national blacklist draw on different sources, such as: those identified through national case law and/ or CJEU rulings or those flagged by consumer enforcement authorities.

However, trader associations and some individual traders (e.g. platforms, marketplaces) mentioned that their preference was for greater harmonisation of contract terms to ensure that consumers are protected on a uniform basis against unfair standard contract terms through approximation at EU level of the national blacklists. The rationale for this was that many traders operating in the digital environment operate cross-border and/ or are highly internationalised. Therefore, they identified a risk of the regulatory environment becoming fragmented with divergent contract terms prohibited and classed as unfair in different countries, which could lead to a complex legal landscape and contradictions as to which contract terms were seen as being unfair. A global marketplace commented that they would prefer harmonised unfair standard contract terms and less divergence. A legal academic pointed out though that this may not be feasible due to the national character of contract law.

Such divergence could in the view of traders interviewed undermine the single market, given the cross-border nature of their operations and of many transactions conducted in the digital environment. However, other stakeholders such as legal academics interviewed pointed to legal barriers to bringing about greater harmonisation in contract terms, namely the fact that contract law is a national competence, with a complex and fragmented regulatory landscape.

Reference should also be made to Section 3.4.2 on internal coherence (EQ16). Section 3.4.2.8 considers how far these are advantages and drawbacks due to that fact that the UCTD is a minimum harmonisation Directive whereas the UCPD and CRD are maximum harmonisation Directives. The overall findings were that:

- The minimum harmonisation nature of the UCTD remains more realistic given that contract law diverges across the Member States because it remains largely national in character.
- There is already adequate scope for Member States to have the necessary flexibility to prohibit contract terms that emerge in a national context through the development of national blacklists. However, the legal framework would be more effective if some of the contract terms identified as unfair and non-transparent at national level were integrated into an EU-level blacklist of such practices to ensure reasonable commonality across the EU-27 and to prevent the emergence of cross-border barriers to trade.

3.4 Coherence

An evaluation should look at how well an intervention works internally (internal coherence) and the degree of coherence with other EU (regulatory) interventions (external coherence). In the context of this fitness check, internal coherence has been analysed at two levels, firstly the extent to which the legal text of each of the three Directives is coherent, and secondly, the degree of coherence between the three Directives. External coherence can be defined as the extent to which there is coherence between EU consumer law and other relevant EU laws, especially digital and data-related legislation, but also more broadly, such as audiovisual media.

3.4.1 Methodology for assessing internal and external coherence

An explanation of the methodology for assessing internal and external coherence is first provided.

Regarding **internal coherence**, the extent to which any internal discrepancies and/or inconsistencies between the provisions of the three Directives within study scope, (the UCPD, UCTD and CRD, as modified by the Modernisation Directive) was analysed. The focus was on assessing any specific provisions related to transactions and practices in the digital environment, of which there are only a few, mainly stemming from the MD's recent regulatory amendments to the underlying legislation. In addition, any inconsistencies in relation to the legal framework overall were assessed, given that many digital practices are regulated through general provisions.

The assessment was mainly based on desk research and stakeholder consultations, especially interviews, and an analysis of closed and open responses to the targeted consultation.

Regarding **external coherence**, the assessment considered the extent to which there was evidence of any **inconsistencies, duplication, loopholes or legal gaps** regarding the inter-relationship between EU consumer law and other relevant legislation from the perspective of achieving digital fairness. The assessment necessarily goes however beyond a legalistic exercise alone, as often the terms without prejudice to other applicable legislation are mentioned in legal texts. Stakeholder perceptions on the overall coherence of the legal framework were considered drawing on the feedback received through interviews, the public consultation and targeted consultation respectively. Earlier position papers in response to previous EU legislative initiatives, such as the DSA, DMA, AI Act, EU Data Act, etc. were also considered where relevant as these sometimes touched upon coherence issues potentially relevant from an EU consumer law updating and modernisation perspective. As much of the feedback on coherence pointed to interesting issues but without providing technical detail, the assessment of external coherence relied heavily on additional desk research to complement the consultation feedback.

3.4.2 Internal coherence

EQ16 – Can any internal discrepancies and/or inconsistencies between the provisions of the Directives related to transactions and practices in the digital environment be identified?

Are there any further internal coherence-related issues across the three Directives be identified, for instance from the perspective of EU consumer law combining both minimum and maximum harmonisation directives?

The extent to which there are any internal discrepancies and/or inconsistencies between the provisions in the three Directives (the UCPD, UCTD and CRD, as modified by the Modernisation Directive) related to transactions and practices in the digital environment was analysed.

Given the technology-neutral and general principles-based approach that underpins EU consumer law, two out of the three Directives (the UCPD and UCTD) include the general principle-based approach that has secured longevity of these two legal instruments. They do not separately cover transactions and practices in the digital environment, which are already included within the general provisions, with examples of how the law should be applied in a digital context being provided instead in the Guidance of the European Commission on each of these Directives.

As there are relatively few provisions specific to the digital environment except those relating to distance contracts in the CRD and a small number of digital-specific provisions introduced through the MD, it is instead left to national courts to interpret the general provisions of the UCPD and UCTD in the digital environment. Accordingly, there are relatively few internal coherence issues.

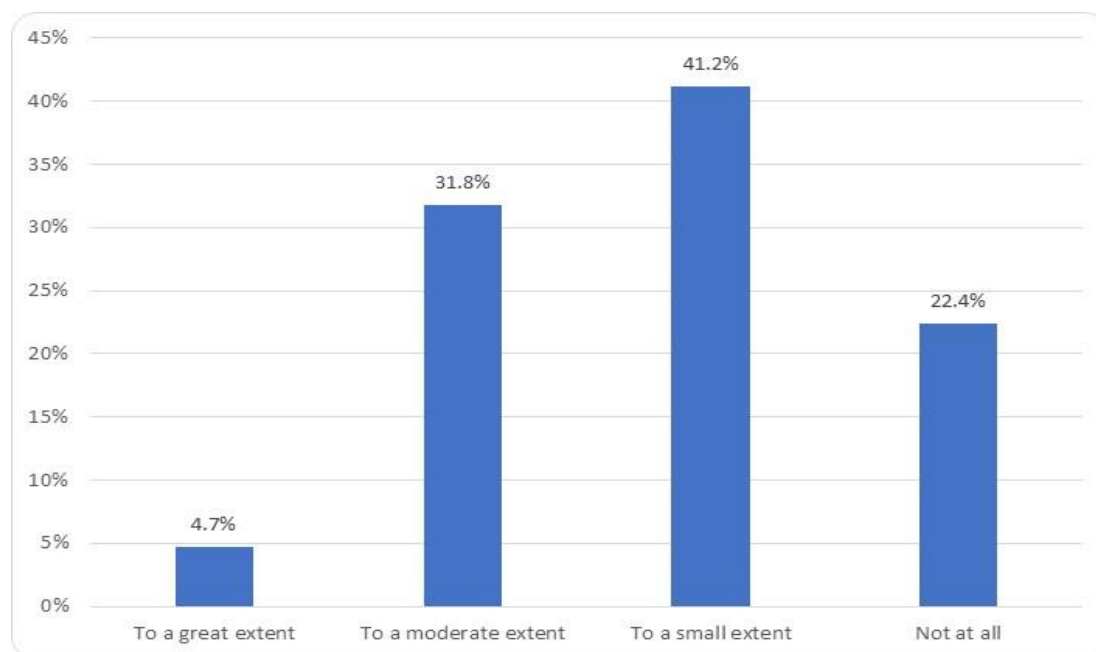
Whilst some issues are legalistic, others relate more to the relationship between the relevance and coherence criterion, as for instance, developments in technologies may mean that provisions remain partially relevant, but there could be a case for further updating to ensure ongoing relevance and coherence.

3.4.2.1 Survey feedback on internal coherence

Whereas the first sub-question considered the internal coherence of the specific provisions of the Directives related to transactions and practices in the digital environment and whether these were coherent across the three laws within scope, there are a number of broader evaluation issues that relate to general perceptions of coherence (i.e. drawing on the survey data) and to strategic issues such as whether the regulatory approach overall is working well, for instance, how far it remains coherent for the EU consumer law *acquis* to consist of a combination of minimum and maximum harmonisation Directives.

Findings from the targeted consultation as to perceptions of internal coherence among stakeholders is first provided. Responses from the public consultation are also considered, but under external coherence:

Figure 3.32 – To what extent are there internal inconsistencies, overlaps or gaps between the provisions of the three EU consumer law Directives in the digital environment? (n=85)



Source: targeted consultation

There were not generally perceived as being any major inconsistencies between the different pieces of consumer legislation and therefore no general coherence problem. Regarding the findings in the targeted consultation as to how far stakeholders viewed there as being **any**

inconsistencies, overlaps or gaps between the provisions of the three EU consumer law Directives, 22.4% stated not at all, 41.2% to a small extent, 31.8% to a moderate extent and only 4.7% to a great extent. It should be noted that there was a high proportion of ‘don’t knows.’ These were taken out of the graph to ensure a clearer picture among those expressing a view.

As outlined in Section 1.4.3 (intervention logic), whilst the three pieces of EU consumer law concerned share the same general objectives, their specific objectives differ. The differences in the specific objectives between the three Directives are sufficient to avoid any major overlaps or inconsistencies, as the legislation was designed to achieve different. However, some **technical inconsistencies were identified**. Examples are now provided in this regard.

3.4.2.2 The interplay between the UCPD, CRD and the UCTD and the accompanying guidance

Under the effectiveness-related EQs, stakeholder feedback was that there has been a positive reaction to the important role of guidance in providing interpretation and case law examples of what types of practices are prohibited. Whilst guidance was welcomed, according to some legal academics, there is a risk that legal uncertainty may emerge over time as the Guidelines are non-legally binding and their interpretative character may, on occasion, push the boundaries of legal doctrine.

Guidelines have practical relevance but given they are not sources of law, and their influence is contingent to an extent on their persuasiveness. Even if they closely refer to the legal provisions and mention case law, they still provide interpretation of the applicability of the general principles in particular contexts, for instance in relation to business practices. It would arguably be more coherent if the Commission were able to consolidate the content of the Guidelines into the related legal instruments in some areas, such as to codify some more specific digital provisions.

Examples are that in the UCPD Guidance, it is already made clear that dark patterns are prohibited under the general provisions, but there are no specific rules in the UCPD regarding any digital provisions in relation to regulating dark patterns in online design interfaces. A further example is that the importance of transparency in real-world equivalent currency within video games when purchasing loot boxes that provide users with access to virtual items or virtual currencies is mentioned in the Guidance, but not in the legislation itself.

3.4.2.3 The CRD

There are some **digital-specific provisions in the CRD applicable to distance contracts**. Examples are:

- The **obligation to pay (Article 8 (2) - Formal requirements for distance contracts)**. Pre-contractual information requirements relating to the final stage in the transactional process. When consumers enter into a distance contract, the trader must ensure that, when placing their order, the consumer explicitly acknowledges that the order implies an obligation to pay. There is a strong digital element, as the trader must provide a prominent button where the consumer confirms acceptance of their obligation to pay.
- The **new right of withdrawal button that is being integrated into the CRD applicable to all contracts**, following the recent adoption of Directive 2023/2225 on distance financial services for consumers. This will require traders to ensure that a withdrawal button is designed into their website or online interface. Whilst emanating from financial services-related legislation, this will be made applicable to all sectors.

There was **some stakeholder feedback regarding these provisions from a coherence perspective**.

The importance of maintaining the ongoing relevance of certain legal provisions through future-proofing (e.g. by ensuring that provisions remain suitable for all types of traders, and across all types of platforms, apps and devices) was mentioned.

The CRD's Art. 8(2) requires traders to include a button for consumers to acknowledge they understand the obligation to pay. However, this implies transactions being conducted on a website or app with a screen. The prevalence of screenless devices and voice-activated transactions raises issues as to whether legal provisions also need to reference alternative means for consumers to confirm they understand the obligation to pay, such as the possibility confirming via voice.

Some stakeholders perceived the right of withdrawal button to be potentially onerous, especially for SMEs. Some EU industry associations representing the interests of the e-commerce sector were not in favour of a RoW button. However, consumer organisations pointed to challenges for consumers in exercising their RoW due to dark patterns in interface design, and pointed to overly cumbersome steps to apply the RoW. The coherence perspective is whether the recent inclusion of a RoW button in 2023 should by the same logic result in changes being made to the CRD to incorporate a cancellation button to ensure it is as easy to exit as to enter contracts (subject to a minimum notice period). This principle is already included in the UCPD Guidance (also mentioned in the DSA – see external coherence).

Similar arguments were made by trader associations as to those relating to the obligation to pay around the need to future-proof the requirements as it will not be feasible for all types of interfaces to click a button to exercise a consumers' rights.

The right to a **standard rate telephone number (Article 21 - Communication by telephone)**. This is also relevant for transactions conducted digitally.

The standard rate telephone number previously covered all sectors. Following the MD, it has now been extended to cover all **passenger transport services, thereby strengthening coherence**. As all sectors are now covered, this is an example of how legal loopholes have been closed. However, there are instead considerations as to whether from a general coherence perspective, it would make sense to include references within the legal provisions to a wider set of means through which traders and consumers communicate in the digital environment.

The focus on phone contacts between traders and consumers rather than other communications means could be regarded as outdated. A more coherent approach could be to ensure that a further communications means are referenced relevant to the digital age. By 2024, it became common for **consumers to interact with traders through AI chatbots and human chat interfaces** to answer queries, address complaints and access customer services. These communication means could become the most common means of communication between consumers and traders, whereas the legal framework tackles an issue that only relates to a single communication media, interactions between traders and consumers via (standard rate) phone calls. Here, there is a connection with the AI Act as AI chatbots are allowed, although users must be made aware that they are interacting with an AI bot. It would **arguably make the legal framework more coherent and consistent if in addition to the right to access a standard rate telephone number, there were the right to interact with a human interlocutor**.

A **potential loophole** regarding the application of the right to a standard rate telephone number that could undermine coherence (or at least the effectiveness of Art. 21, CRD) is that traders may theoretically be compliant by providing a phone number charged at the basic rate but then have insufficient customer services representatives to answer the calls within an acceptable timeframe. For instance, there are examples in the travel sector of calls being unanswered for 45 minutes or more until consumers hang up, although there is sometimes

the option in parallel of contacting customer services via an online chat interface. The possibility of requiring traders to adhere to **minimum standards in telephone service provision could be considered, such as answering a call within a minimum of 15 or 20 minutes**, and/ or the **right to a callback during especially busy periods**. This could benefit consumers and avoid ineffective application of the law.

Under **Article 16(m)- Exceptions from the right of withdrawal (RoW)**. The MD allows traders to ask consumers to forfeit their RoW in contracts for the supply of digital content under certain conditions in contracts for the supply of digital content.³⁸¹ This effectively means asking consumers to 'opt out' of the RoW for digital content for content downloaded onto tangible media. Some traders were concerned that this may undermine coherence as it raised the issue why given consumers theoretical rights if they are then asked in the case of digital content to opt out of those rights. However, this is specific to the nature of digital content which once downloaded is difficult to give back without the trader being able to ensure that the content is not consumed. However, traders expressing concerns did not provide alternative suggestions as to how to make the legal framework more coherent.

A coherence issue identified in the earlier 2017 Fitness Check was **legal incoherence within the CRD**, as the pre-contractual information requirements and right of withdrawal applied to the free provision of digital content, but not to the "free" provision of digital services, thereby creating legal uncertainty for both users and providers. However, this was addressed through the MD, which extended the RoW to free services.

A further coherence issue was identified through the previous Fitness Check which analysed the interaction and **possible overlap between information requirements in the UCPD's Art. 7(4) and the CRD's Art. 5 and 6**. Further details are now provided:

The UCPD's Art. 7(4) contains information requirements for the "invitation to purchase" of specific products at a specific price. These apply already at the advertising stage, whilst the CRD includes the same but also more detailed requirements at pre-contractual stage (i.e. immediately prior to the consumer entering into a contract). Consequently, traders may have to provide some of the same information in advertising (e.g. in the ad displayed on an online newspaper) they are required to provide once again at the pre-contractual stage (e.g. on the pages of their online web-shop).

This issue was already investigated in 2018 through the IA of the MD. Whereas some traders viewed this requirement as burdensome, consumer associations were strongly against watering down pre-contractual information requirements. This option was subsequently not pursued in the final text of the MD. This issue was mentioned by a few traders in interviews and in some online survey responses from traders and their representative associations, under questions relating to possible measures to help simplify the regulatory framework by eliminating possible duplication in information requirements. However, arguably this information is required for different purposes at different stages in the transactional process, as per the findings set out in the IA of the MD.³⁸²

Moreover, the Fitness Check from 2017 (Part 1, pg. 166) notes that there are differences in the type of information to be provided under the CRD and UCPD respectively as *"the amount of information that must be provided at the precontractual stage (under Article 5/6 CRD) is clearly more comprehensive than that required in the context of an invitation to purchase (under Article 7(4) UCPD). Moreover, Article 5/6 CRD takes a minimum harmonisation approach, which means that Member States can maintain or introduce additional*

³⁸¹ The conditions are if the content has been delivered through a tangible medium and the performance of digital content has begun. This is only in instances where the consumer has given their prior express consent to start the service during the period of right of withdrawal or has acknowledged that he is thus losing his right of withdrawal or where the professional has provided confirmation of the contract on a durable medium.

³⁸² See pg. 28 of Part 1 of the SWD on the IA of the MD (SWD(2018) 96 final), Driver 3: Overlapping and outdated information requirements).

precontractual information requirements; this is not possible under the full harmonisation approach of Article 7(4) UCPD". A further point raised in the fitness check was that awareness among traders regarding Article 5/6 in the CRD was higher among SMEs than awareness about Article 7(4) UCPD, linked to the positive information duties under Article 5/6 CRD. These were considered to be easier to prove as there is no transactional decision test (unlike under the UCPD).

Regarding the **transparency of search rankings** in the CRD (as amended through the MD), a consumer association in Germany raised questions regarding the coherence of new rules to strengthen the transparency of rankings in the CRD targeting online marketplaces but not to other types of traders. The association raised concerns regarding coherence if transparency requirements only apply to online marketplaces and not to all platforms providing consumers with the possibility to search for products and services as in the UCPD.

3.4.2.4 The UCPD

Changes to the UCPD made through the MD have strengthened coherence by partially addressing the relationship between platforms, traders and consumers for the first time, which is also a challenge addressed through the DSA, given that the traditional focus in the consumer law acquis e.g. in the CRD and UCPD has been on regulating the transactional relations between traders and consumers. More specifically, Article 7(4)(f) UCPD considers as material the information regarding whether a third-party making goods or services available on a marketplace is a trader or not. This has addressed a legal gap as consumers previously did not have information whether they were purchasing from an individual or a trader.

The UCPD does not explicitly regulate which types of personal data can be used for personalised advertising. The prohibition of the use of personal data for psychographic profiling was identified as a problem in the case study on personalised advertising. Some stakeholders raised concerns about this in their public consultation position papers and targeted consultation as there is the risk of manipulating consumers in a way that exploits their weaknesses. The UCPD has an effect-based approach when applying its general tests. Accordingly, it is not about knowing a person's emotional state *per se* - but rather what is done with that information. A related challenge in the view of some legal academics, was therefore how to operationalise the UCPD's concept of "undue influence" thereby addressing the widespread concern that online environments (but not only) can be highly manipulative but also exercise undue influence on consumers, especially vulnerable consumers.

Although the guidance touches on personalised ads, the lack of explicit Articles concerned with data risks creating legal ambiguity for traders as to whether certain practices such as psychographic profiling are prohibited or not. It would arguably strengthen legal clarity if the limitations in the use of personal data, such as was also mentioned in the UCPD.

Consistency of information requirements for complaint handling systems in the UCPD and the CRD. A Ministry in Austria noted that it was not fully clear why the information requirement pertaining to complaint handling systems in the UCPD (Art. 7 para 4 (d) UCPD) was deleted because of the Modernisation Directive, but a similar sub-Article remains within the CRD. The updated UCPD Guidance (2021) explained: "*That information is most relevant at the pre-contractual stage, which is already regulated by the CRD, and therefore the requirement was not needed for invitations to purchase at the advertising stage under the UCPD.*"

Updating the UCPD blacklist to reflect developments in data protection legislation. A minor point but relevant to updating the legislation to ensure consistency is that Annex 1 of the UCPD (commercial practices which are in all circumstances considered unfair), includes an **outdated reference under point 26 to the Data Protection Directive 1995**, instead of

the **GDPR 2016**.³⁸³

3.4.2.5 Relationship between the UCPD and UCTD

Firstly, regarding the **coherence between the UCPD and the UCTD**, after the adoption of the UCPD in 2005, the relationship between these two European Directives had remained unclear. The UCPD, in Article 3(2), identifies that its provisions are without prejudice to the contract law, pointing out that the legal framework of the UCPD is not supposed to interfere with contract law. Nevertheless, it has been clear including through jurisprudence that there is a strong interlinkage between the UCPD and the UCTD. This was confirmed in the judgement of the CJEU in Case C-453/10 *Pereničová*.³⁸⁴ In *Pereničová*, the CJEU confirmed that, firstly, the fact that a trader resorted to an unfair commercial practice is one of the elements to be considered in the assessment of unfairness of contractual terms under the UCTD. Second, this fact has no direct effect on whether the contract is valid under the UCTD, without prejudice to any national rules pursuant to which the contract entered into on the basis of unfair commercial practices is void as a whole. The CJEU has not ruled directly on whether, in reverse, the use of unfair contract terms under the UCTD is to be regarded as an unfair commercial practice under the UCPD. This is something that could be addressed in the future, were the text of the UCPD to be updated and revised.

Moreover, the transparency requirements are one of the instruments of EU consumer law designed to address power imbalances between consumer and trader. The UCTD was the first European legal instrument to introduce the transparency requirement of contract terms in consumer contracts. Under Article 5, such terms must be drafted in plain, intelligible language, which must be assessed on a case-by-case basis. However, what was missing for years from the UCTD rules is a benchmark against which the transparency assessment should be assessed. The CJEU has again clarified what the benchmark is to be used, for example in its decision in Case C-26/13 *Kásler*, by referring to the average consumer for the assessment of transparency requirements. In other words, the national courts should use the standard of the average consumer for the assessment of the transparency requirements. This is something that could be codified in the future version of the UCTD to improve coherence with the UCPD, which also refers to the average consumer, and align with CJEU interpretation.

Importantly, a legal academic responding to the targeted consultation pointed to an **inconsistency in the UCTD in comparison with the UCPD**³⁸⁵ 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'** (explored in detail in the key concepts section of conceptual framework and in the case study on consumer vulnerability).

The research paper cited by the respondent makes clear that in the UCTD, (1) the system of EU law requires the transparency of a term to be assessed from the perspective of vulnerable consumers and (2) the more demanding standard shall be used when the average consumers operating on the market do not offer herd protection to the vulnerable consumers. However, this regulatory approach was seen as having some weaknesses as *"the premise relies on the faulty assumption that vulnerable consumers are protected when core terms are transparent for the average consumer."* In the view of the authors, demanding core terms to be transparent for the vulnerable consumer in those circumstances contributes to reaching a high level of consumer protection.

³⁸³ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02005L0029-20220528>

³⁸⁴ Case C-453/10. Consumer protection — Consumer credit agreement — Incorrect statement of annual percentage rate of charge/ Effect of unfair commercial practices and unfair terms on the validity of the contract as a whole.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0453>

³⁸⁵ The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration (2022), Esposito, Fabrizio and Grochowski, Mateusz, European Review of Contract Law (ERCL), Vol. 18, No. 1, pp. 1-31, April 2022, Max Planck Private Law Research Paper No. 22/11 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4109474

In the **UCPD**, transparency plays a key role in relation to misleading practices which are focused heavily on consumer information problems.

Given that digital markets and services are data-driven, in the digital era, the **UCPD's coherence could be strengthened if the interaction with the GDPR and rules on personal data and privacy were made clearer**, either in the legal text or in guidance, for instance in respect of personalised advertising and profiling. The potential misuse of personal data which could then lead to manipulative practices is not explicitly mentioned, which arguably undermines coherence. A legal academic commented however that caution is needed as to how the use of data and its interaction with consumer law is regulated. "The point is not the consumer knowing the information that is being used; the point is the consumer being protected from using *any* information to their detriment. Hence, transparency for consumers about what is being used is not the solution. The solution is transparency for traders about what they cannot do".

3.4.2.6 Strengthening the UCTD's coherence

The UCTD provides a somewhat fragmented protection of consumers in consumer contracts. The scope of protection of the UCTD was substantially developed through a rich jurisprudence of the CJEU. A trader association in the audiovisual sector (ACT) responding to the targeted consultation pointed to the need to provide additional regulatory clarity to improve consistency in the application of the UCTD and interpretation of its rules. In the RWE Vertrieb case³⁸⁶, they noted that the CJEU ruled on the legality of a price variation clause for the supply of natural gas, which has implications for these types of clauses, including Pay TV and subscriptions. The case clarified transparency requirements regarding price changes in longer-term contracts and reiterated the obligation of the use of plain and intelligible language and transparency.³⁸⁷ The CJEU has made rulings as to what is required for contract terms to be considered plain and intelligible both in reviewing this case and in its wider rulings.

Some national members of the trade association support the issuing of further Commission guidance on the UCTD regarding **price variation clauses in easily cancellable contracts of indeterminate duration for non-essential or financial goods and services**. The objectives would be to:

1. Clarify how the list of exemptions in point 2 of the annex should be understood in relation to point 1 of the Annex.³⁸⁸
2. Specify that a case-by-case assessment is needed regarding transparency obligations and the circumstances listed in Article 4(1) UCTD.
3. Include examples of contracts that may be subject to more flexible transparency requirements.
4. Clarify that the option to cancel a contract and easily move to another provider are important factors to consider when assessing the potential unfairness of a price change clause.
5. Provide examples of circumstances that should be considered when assessing the unfairness of a price variation clause.

In the view of a legal academic responding to the targeted consultation, clearer rules are needed on how to apply Art 4(2) UCTD.

³⁸⁶ RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV (2013) C-92/11 is an EU law and consumer protection case, concerning the UCTD. *ECLI:EU:C:2013:180*

³⁸⁷ See <https://dare.uva.nl/search?identifier=ff43892d-a589-44a1-8f86-90cb7c1e126f>

³⁸⁸ Annex 1 sets out the terms referred to in Article 3 (3), "terms which have the object or effect of" whilst Annex 2 determines the scope of subparagraphs (g), (j) and (1).

The issue was addressed by the CJEU, for example in Case C-26/13 *Kásler* concerning so-called “core” terms related to the price, as regards their transparency and fairness in light of Article 4(2), that exempts the terms relating to the main subject matter of the contract or the adequacy of the price and the remuneration from the fairness assessment provided they are drafted in plain intelligible language. The specific case pertained to consumer credit contracts denominated in foreign currency and the fairness of the terms relating to the exchange rate (the difference between the rate of exchange applicable to the advance of the loan and the selling rate of exchange applicable to its repayment).

A further legal academic commented that this issue is often the subject of preliminary references by national courts and some consider that CJEU decisions on this matter have not been fully consistent (c.f. Dziubak and Lombard).³⁸⁹ A core issue raised is whether the contract can continue without a price (e.g. a free loan). If the EU legislators were to definitively say 'yes', most national case law would not be relevant anymore (and banks would become more careful and conservative).

3.4.2.7 Role of the Modernisation Directive in strengthening internal coherence

The Modernisation Directive has partially adapted the existing EU Consumer law to the particularities and challenges of the digital market and economy. Through the MD, there are a few new specific requirements relevant to transactions and practices in the digital environment as an adaptation of the legal framework to address requirements in the digital age was one of the reasons for passing the MD. The MD has included four new types of commercial practices as those that are always automatically prohibited. The extent to which the MD's adoption has strengthened coherence and eliminated inconsistencies, duplication and loopholes was considered, as well as whether there are any outstanding gaps. For example:

- **There are enhanced rights for consumers through the extension of the RoW to include free digital content and services.** In the context of the data-driven digital economy, the MD has strengthened the coherence of the underlying CRD by closing a loophole that previously differentiated between paid-for and unpaid products and services. The right to withdraw does not automatically entitle consumers to the 'right to be forgotten' (i.e., traders deleting any personal data they have collected due to said free service). However, considering that data collection is part of the business model for such services, according to a legal academic contributing to the study, “the right to be forgotten should automatically apply, as the functional equivalent of the price reimbursement.”
- The MD introduced the first common European rules related to the online reviews that consumers in the digital age increasingly rely on. Under the MD, **fake reviews, the manipulation of reviews and soliciting the services of people that provide such reviews have been prohibited.** There was also a requirement introduced for traders to take steps to check that consumer reviews are genuine by verifying their authenticity (see **Art. 7.6 - misleading omissions**, Annex 1 blacklist, point 23b and c). The only coherence issue that emerged is whether all traders should be required to do more on consumer reviews, given the present focus on marketplaces and platforms (i.e. mainly large firms).
- Whilst understandable that there are concerns about administrative burdens, it would appear **incongruous that platforms are required to take steps to prevent and monitor fake reviews, whilst SMEs/ smaller e-commerce players are under no**

³⁸⁹ See <https://www.degruyter.com/document/doi/10.1515/ercl-2020-0030/pdf> and <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals%5CEuCML%5CEuCML2022037.pdf>

such obligation. As many large online marketplaces interviewed only allow reviews or comments to be left on goods or services purchased by validated consumers that have already made a purchase. Therefore, outstanding problems may arguably lie more with smaller e-commerce players. Although these may lack resources to perform such checks, the volume of consumer reviews that they would need to check would be significantly lower compared with large marketplaces.

As noted earlier under the CRD sub-section, some stakeholders raised similar issues that it was inconsistent that the **transparency of search rankings is required of online marketplaces** but not for other types of traders unlike the UCPD, which is applicable to all traders.

Regarding **personal data**, the CRD (as amended through the MD) includes a definition of personal data and new obligations to comply with the GDPR if a consumer withdraws from a contract. Specifically, under Art. 13 – Obligations of the trader in the event of withdrawal, **Art. 13(4)** states that *“in respect of personal data of the consumer, the trader shall comply with the obligations applicable under Regulation (EU) 2016/679”*. Consumers have the right to ask for their data to be deleted following the RoW. In the case of free services, some legal academics have argued that this should be automatic (asking consumers to opt out from data cancellation should they so wish but otherwise traders could be obliged to delete data once a consumer has withdrawn from a contract).

There could however be an argument that to strengthen coherence across all EU consumer laws by including references to relevant EU data protection legislation, at least in the recitals, but also possibly in certain provisions. For example, there is presently a lack of references to the GDPR in specific areas e.g. to Art. 9 GDPR as concerns the use of sensitive data and its relevance under the UCPD for personalised advertising.

3.4.2.8 Maximum and minimum harmonisation character of different pieces of EU consumer law

Whereas the UCPD and the CRD are maximum harmonisation Directives, the UCTD and PID are minimum harmonisation in character. Part of the reason is that there has been a shift over time in EU consumer law from minimum towards maximum harmonisation Directives. For minimum harmonisation, a directive sets minimum rules and EU Member States can set higher rules on top of those established in the EU legislative act. In the case of maximum harmonisation, EU Member States may not introduce rules that are stricter than those set out in EU law.

In our assessment, the extent to which there are any coherence issues stemming from the divergence between directives in their approach to harmonisation was considered. This issue was raised during the interview programme by some stakeholders (including some legal academics, trade associations and some ministries of the Member States). However, it was not seen as the most important issue in respect of digital fairness but was rather a general issue relevant to examining the overall coherence of the consumer law acquis.

Some trader stakeholders pointed to the **incongruousness from a single market perspective of retaining the minimum harmonisation character of the UCTD**. They pointed to a risk of national regulatory divergence in the UCTD blacklist of prohibited practices, which is drawn up by national ministries in their capacity as competent authorities.

However, there would also be potential barriers to adopting a maximum harmonisation approach under the UCTD. When the Directive was first drafted, minimum harmonisation in consumer law was the prevailing model. However, there were more specific reasons why the UCTD was drawn up as a minimum harmonisation directive. *“The fact that unfair contracts regulation is connected to deep cleavages between the Member States in their conception of the role of contract law would have made it difficult to pursue maximum harmonisation, which*

would have brought with it a need for further harmonisation of contract law as well. For example, the huge variety of national mandatory rules on various issues and contract types would have had to be scrutinised to check that their protection level did not rise higher than the Directive would allow".³⁹⁰

During the present study, some stakeholders interviewed noted the complex interplay between the UCTD on unfair standard contract terms and national laws, given the fact that contract law is mainly national. Some legal academics, such as in the study above on *Rethinking EU Consumer Law* have argued it is beneficial that the UCTD is minimum harmonisation to allow sufficient flexibility for adaptation to national contract laws.

The **potential benefits of a minimum harmonisation approach in enhancing consumer protection through the interaction between EU consumer law under the UCTD and national contract laws** was noted. For instance, in a 2023 research paper by Loos,³⁹¹ it was noted that the interpretation of fairness benefits from wider rulings by national courts pertaining to national contract laws, not only those specific to the UCTD.

"The Court recently held that the Directive does not preclude a rule of national law that the lack of transparency of a term in a consumer contract automatically leads to a finding that it is unfair. This means that in such case the unfairness test itself is not applied. However, as such a rule of national law automatically qualifies the non-transparent term as being unfair, all consequences that the Court of Justice has attached to the unfairness of the term apply."

Some interviewees pointed to the fact that the notion of minimum and maximum harmonisation across the three Directives is more **nuanced** than it appears at first sight, leading to a blurring in the delineation. For instance, whilst the CRD is a maximum harmonisation Directive, there are some **regulatory choices** that Member States can make, meaning some national regulatory divergence is permitted, even if the Directive is maximum in character. There are several regulatory choices within the CRD, which has the advantage that it retains some degree of flexibility. The Commission publishes this information online. For instance, additional information requirements in accordance with Article 6(8) of the *CRD is one of the regulatory choices, about which the Member States must inform the Commission in accordance with Article 29.*

According to a legal academic interviewed, a concern about EU consumer law is the perceived lack of flexibility within maximum harmonisation directives. However, this problem could be eased in two complementary ways. Their suggestions were, in summary, that:

- a). the Commission could be given new powers to add additional new items to the black and grey lists on a more flexible basis than the current process of making regulatory amendments through amending legislation;
- b) Member States could be given the power to introduce specific bans under a notification system where the Commission must either i) accept the suggestions made by individual MS if these were feasible as regulatory choice; ii. make the suggestions applicable to the whole Union; iii. Reject the proposal.

³⁹⁰ Rethinking EU Consumer Law (2017). Howells, Geraint & Twigg-Flesner, Christian & Wilhelmsson, Thomas. 10.4324/9781315164830.

³⁹¹ Loos, Marco B. M. "Crystal Clear? The Transparency Requirement in Unfair Terms Legislation" *European Review of Contract Law*, vol. 19, no. 4, 2023, pp. 281-299. <https://doi.org/10.1515/ercl-2023-2018>
<https://www.degruyter.com/document/doi/10.1515/ercl-2023-2018/html?lang=en>

Under a mechanism such as that described above, maximum harmonisation Directives could retain sufficient flexibility to prevent concerns regarding “*disproportionate balancing in favour of market integration since it would be relatively easy to make decentralised adjustments of the regulatory framework aimed at addressing new or newly salient consumer protection issues*”.

This example has been included to demonstrate that there are different ideas regarding how flexibility can be retained despite the maximum harmonisation character of some consumer law Directives (e.g. the UCPD and the CRD).

There could however be concerns regarding the potential risks associated with undermining the single market from having any further flexibility to allow scope for regulatory divergence if warranted. As noted earlier in relation to regulatory choices, the CRD has a mechanism similar to the one suggested regarding some provisions, such as information requirements.

Balanced against this, many traders and their representative associations found it would be more coherent to retain strong harmonization to avoid further regulatory divergence. The same is true of the Modernisation Directive, where many of the Articles updated in the underlying EU consumer legislation are required to be transposed into national laws, but there remain regulatory choices to be made (analysed in Part 2 of the study). Examples are that there has been an extension of the RoW for unsolicited visits to 30 days in the case of doorstep sellers. Regulatory choices or options do not in themselves negate the basic maximum harmonisation character of the CRD but illustrates that national divergence in application is permitted within maximum harmonisation Directives.

Research by legal academics has also commented on the **degree to which a maximum harmonisation can be achieved in practice, given obstacles to its achievement**. As mentioned in a paper by de Vries (2011)³⁹², maximum harmonisation can be difficult to achieve given divergence in national legal application and interpretation through national case law, albeit with CJEU rulings providing greater legal certainty across the EU over the longer-term.

“Maximum harmonisation should guarantee that one uniform set of rules applies to the whole EU, thereby contributing to legal certainty and reducing barriers in the internal market. However, the aim for uniformity conflicts with the frequent use of so-called general clauses: clauses that are generally formulated and need further interpretation by the courts. Various national interpretations of these clauses will hinder the aim for one uniform set of consumer laws.”

Some academic literature has pointed to nuances in how far the three consumer law Directives within scope have elements that are minimum and maximum harmonisation in character. For instance, under the UCTD, the degree to which Member States can diverge in its application is limited. “*National discretion is limited to structuring the standard, and the use of an indicative national blacklist of unfair standard contract terms.*”³⁹³ In the same research paper (2017), it is made clear that national laws continue to exercise an influence in the interpretation of the UCPD and UCTD, despite one of these Directives being maximum and the other a minimum harmonisation Directive.

³⁹² Maximum Harmonisation and General Clauses - Two Conflicting Concepts? (January, 2011). de Vries, Anne. Available at SSRN: <https://ssrn.com/abstract=1703078> or <http://dx.doi.org/10.2139/ssrn.1703078>

³⁹³ The Interpretive Function of the CJEU and the Interrelationship of EU and National Levels of Consumer Protection (2017), Geraint Howells and Gert Straetmans, <http://archive.sciendo.com/POF/pof.2017.9.issue-2/pof-2017-0014/pof-2017-0014.pdf>, DOI: 10.1515/pof-2017-0014

“The analysis of national case law relating to unfair contract terms and unfair commercial practices illustrates that national traditional standards continue to play an important role in the assessment of law provisions. This may be seen as self-evident in the presence of a minimum harmonisation directive like the UCTD, which automatically implies broad discretion for the Member States. With regard to the maximum harmonisation brought about by the UCPD, the use of general concepts like the average consumer, as interpreted by the CJEU, also allows room for national divergent applications”.³⁹⁴

Moreover, some academic literature points to the need to **strike a balance between single market and consumer protection objectives** as consumers may **benefit from the interplay between EU law and national law**, for instance due to the protections afforded in both the UCTD and those in national contract law, which may afford extra protection than would otherwise be the case if there were only EU law. In *Rethinking EU Consumer Law (2017)*, it was argued that “*the balance between internal market and consumer protection objectives has swung too much in favour of market integration by overstatement of the case for maximum harmonisation*”.³⁹⁵

Overall, however, there would be some advantages in ensuring that there is a common EU-wide list of standard unfair contract terms in the UCTD. Given that many traders in the digital environment operate either in multiple EU countries or on a pan-European basis, it would be useful to have a common set of contract terms prohibited through a European blacklist. However, as some Ministries appear to favour the status quo, there would need to be continued scope for Member States to complement it with their additional list of unfair contract terms. The Commission could play a coordination role to ensure that the added value of a blacklist is maintained that adds in examples of unfair contract terms identified in the national context.

Conclusions

The extent to which there may be challenges in relation to whether specific digital practices are covered in the existing provisions of the three Directives has been analysed. In particular, the analysis has considered how far there is a clear and coherent legal framework and sufficient clarity as to the scope and delineation of the Directives. The conclusions are summarised in the following box:

Conclusions – general internal coherence issues:

- Overall, stakeholders perceived the legal framework to be coherent, with some technical minor issues.
- There is potential scope to transition towards greater harmonisation through the possible development of a more standardised EU-wide blacklist of contract terms and to move away from national blacklists.
- However, there would also be disadvantages of moving away from the UCTD’s minimum harmonisation character given that contract law remains broadly a national competence.

Specific conclusions

- There are only a limited number of legal provisions that explicitly focus on digital transactions and business practices in the EU consumer law acquis given the focus on general principles rather than regulating specific digital practices.

³⁹⁴ Idem. The Interpretive Function of the CJEU, etc. pg.209.

³⁹⁵ Rethinking EU Consumer Law (2017) Howells, Geraint, Twigg-Flesner, Christian and Wilhelmsson, Thomas - <https://library.oapen.org/handle/20.500.12657/23205>

- However, there are some provisions that are digital-specific especially under the CRD and since the MD, several specific further provisions under both the CRD and the UCPD that are digital-related, such as the transparency requirements through information disclosures for online marketplaces.
- Overall, there appear to be relatively few internal coherence issues compared with the 2017 Fitness Check but this is in part because the Modernisation Directive was an amending piece of law which addressed several legal gaps, inconsistencies, and incoherence in underlying EU consumer law, some of which were digital-specific.
- However, in some instances, there remain minor perceived incoherence and duplication from a trader perspective, such as pre-contractual information requirements under the UCPD Art. 7(4) and the CRD's Art. 5 and 6. However, consumer associations view these requirements as being differentiated steps in the transactional process, even if the information to be provided to consumers at different time points may sometimes be the same.
- There are also arguably some legal gaps that may undermine coherence, including in relation to legal provisions already partially addressed through the MD. Examples are: the prohibition of scalper bots being confined to event tickets only, and responsibility for checking fake reviews lying only with those marketplaces hosting reviews on their websites in an intermediary capacity rather than all traders across different types of digital interfaces, including SMEs).
- There does not appear to be a general coherence problem between the UCTD, UCPD and CRD, but rather some technical inconsistencies.
- There is a risk that legal uncertainty emerges over time since the Commission develops non-legally binding Guidelines which, on occasion, may push the boundaries of legal doctrine. There are some more substantive strategic considerations around the coherence of the consumer law framework, but these relate less to specific provisions and more to the regulatory approach adopted in different Directives (e.g. gradual development of the legal framework over time, with the fact that the UCTD (and PID) is a minimum harmonisation Directive, whereas the UCPD and CRD are maximum harmonisation Directives. These issues are tackled under the next EQ, which considers internal coherence from a more general perspective.

3.5 External coherence

3.5.1 Introduction

The assessment of external coherence examined the inter-relationship between EU consumer law and other relevant EU legislation, including digital and data-related laws. In the previous 5 years, many new legislative developments have taken place, such as the adoption, entry into force and/ or application of the DSA, DMA, Proposed AIA, DCD, GDPR, Data Act, and the revised AVMSD. Additionally, there are regulatory proposals that have not yet become EU law that could potentially impact on the consumer law acquis, e.g. the e-Privacy Regulation to update the e-Privacy Directive. Interestingly, although many of these newly adopted pieces of legislation are not purely consumer protection legislation and, even in some cases, consumers are not explicitly, or hardly, referred to in the legal provisions³⁹⁶. The interplay with EU consumer law is complex as there are multiple different facets. Firstly, the interplay stems from the environment (digital environment in general, online platforms, in particular) such as in the DSA, which regulates very large online platforms and very large online search engines.

³⁹⁶ For instance, the AI Act mainly refers to end-users of AI systems, rather than directly to consumers. although there are benefits for consumers, such as the prohibition of social scoring by the public sector, which could be considered as discriminatory to consumers.

Secondly, the interplay is related to the technology being used, such as in the AI Regulation. Thirdly, the interplay arises from the type of transaction (or obligations), such as data-sharing in the Data Act.

The new legislative instruments do not ignore consumer protections laws. On the contrary, explicit statements recognising the inalterability and preservation of consumer legislation are amply included in the recitals and in the legal provisions. Even more, it is commonplace in these EU laws to emphasise that they are adopted “without prejudice to Union law” which aims to promote consumers’ interests and ensure a high level of consumer protection. In that regard, it is frequent that these newly adopted EU laws declare that they complement consumer protection law. Such a declared complementary interaction does certainly ensure consistency and facilitate the understanding of the interplay between consumer protection laws and the digital laws, as listed above. Nonetheless, lack of coherence is not totally prevented by a “without prejudice to” formula. Terminological consistencies, and more substantially, material consistencies may still perpetuate. Hence, despite the intended complementary relationship, in practice, coherence may not be fully achieved. As the various EU laws have different goals, complementarity may not always be in evidence or indeed straightforward. Therefore, external coherence must be assessed beyond the general acknowledgement of no-contradiction and complementariness.

The number of pieces of legislation, with their own policy goals, adopted increases the risk of incoherence, duplications, gaps, or conflicts. The increased number of EU laws that interact with EU consumer law has resulted in increased complexity in application. There is consequently a need to ensure that the legal framework does not lead to any inconsistencies, duplication or loopholes and legal gaps. As such, there is a relationship between the coherence and relevance evaluation criteria, as legal gaps were considered under the latter, as gaps could also undermine coherence.

EQ17 – As far as business-to-consumer (B2C) transactions and practices in the digital environment are concerned, are there any overlaps and / or complementarities between the Directives and any other Union legislation with similar objectives?

This EQ assesses external coherence i.e. the inter-relationship between EU consumer law and other relevant EU legislation.

Various issues identified through the research were found to be relevant when assessing the coherence between the EU consumer law framework and wider EU laws. The following points provide important context:

EU consumer law has evolved over three decades, whereas many digital and data laws have been updated much more recently (though some of the earliest digital and data-related laws stem back to the mid-1990s and early 2000s). Moreover, these different areas of law evolved somewhat separately with different traditions as to how to achieve the intended regulatory objectives.

Ensuring the complete coherence of EU consumer law with other pieces of EU law is challenging given the gradual accretion over time of relevant EU laws that provide consumer protection or that has the (direct or indirect) aim, or effect, of promoting consumers’ interests and ensuring a high level of protection. These include EU consumer law, sectoral law with a consumer protection dimension, digital law, data law and other pieces of law.

Different laws were drawn up during different time periods. Some laws give greater attention to regulating the digital environment than others. Given the rapid evolution in digital markets and services, the concerns of regulators today to ensure high levels of protection for consumers across different types of digital markets and services are different from when the different EU consumer laws within scope were drawn up.

Relevant EU consumer law evolved over a long period since the early 1990s. The UCPD and UCTD were adopted in 1993 and 2005 respectively. This pre-digital era many more recent developments in digital markets and services, such as the advent of the subscription and platform economies. This poses challenges to ensure full coherence across the legal framework, given that some areas of EU law are themselves either relatively or very new e.g. data and digital laws.

Moreover, the legal framework for EU consumer law was designed to be technology-neutral and applicable in an omnichannel environment. This meant that the UCPD and UCTD did not expressly regulate through specific provisions particular business practices relating to transactions in the digital environment and relied on the general principles-based approach.

In contrast, more recent EU legislation (e.g. the DSA, DMA, AI Act) was designed to provide a strong regulatory framework to ensure high levels of consumer protection in the digital age. Laws adopted more recently reflect developments in new technologies and in business practices across different digital markets and services. Moreover, some new rules aim to tackle specific problematic practices in the digital environment, whereas EU consumer law faces the challenge that the rules need to be applied both online and offline. This shows an increasingly visible trend in EU legislation with the adoption of more specific rules that are focussed on problems or challenges raised by emerging technologies, or digital practices. Instead of relying on a general functional-equivalence principle and a technology-neutrality approach, some EU laws aim at addressing specifically these practices. The rules on platforms in the DSA, compared to the rules on intermediary services in the ECD, are illustrative of these trends. Despite its regulatory character, the (proposed) AI Act is paradigmatic in addressing specific challenges of “AI systems” as defined thereby and within its scope. Even the revision of the PLD (a Directive from 1985) to accommodate to digital challenges, including AI systems, is revealing in the same sense.

There has been a general trend towards the adoption of more specific rules in EU law, whereas EU consumer law – at least for the UCPD and UCTD – remains focused on the general principles-based approach and application of a fairness test on a case-by-case basis. This does not imply incoherence, as both regulatory approaches are valid, but makes it more challenging to ensure complete coherence as rules differ in approach, extent, or level of granularity.

EU laws also reveal a general trend towards more complex, longer, elaborate, and detailed legislative texts. A simple comparison between the ECD adopted in 2000, and backbone of the regulation in the Union of digital services for years, and the DSA transpire the different drafting and law-making approaches. Perceived coherence is affected as well by these “style” determinants.

Impact on consumer protection can be indirect and incidental where EU laws are not consumer-directed legislation but have the aim of enhancing fairness, transparency, or the contestability of digital markets. In such cases, the need for external coherence might not be so pressing. However, from a policy perspective, all these pieces of legislative contribute to aligned goals. Coherence is still desirable. As a token of illustration, the P2B Regulation is clearly directed to professional users and aims to alleviate the frictions in the platform economy and mitigate the effect of economic dependency on platforms of professional users providing their products or services to consumers (P2B and B2C relations). It is not “consumer legislation” but it has a positive impact on fairness, transparency, and disputability what may deploy spillovers on consumer welfare.

When new pieces of legislation are adopted, these may not always be fully consistent, coherent, and complimentary as they emanate from different Directorate Generals (DGs) responsible for different policy and regulatory areas, even if there are inter-service consultations aiming to avoid incoherence.

Legal academics and trader associations point to the growing complexity of the overall body of applicable EU legislation due firstly to some issues covered in more than one piece of law and secondly to the increased frequency of regulatory changes experienced by traders in the digital environment.

General coherence of the EU legal framework

Whereas the next section considers the inter-relationship between EU consumer law and selected EU law, there was some general feedback on coherence-related issues worth considering.

EU consumer law was found to be generally coherent with other EU legislation in terms of the legal inter-relationship. This is due to there being some explicit provisions that explain the relationship between EU consumer law and other pieces of law. For instance:

- The application of other relevant laws that provide consumer protection is *without prejudice* to the applicability of existing consumer laws. It is made clear that the application of other legislation such as the DSA is *lex specialis*³⁹⁷ in relation to the generally-applicable framework, i.e. does not negate traders being required to comply with the UCPD's general principles-based clauses. Along the same lines, the (proposed) AI Act states that its rules should be without prejudice to existing Union law, notably on data protection, consumer protection, (...), and product safety, to which the Regulation is complementary. Likewise, the Data Act clarifies that its complements and is without prejudice to Union law which aims to promote the interests of consumers and ensure a high level of consumer protection.
- The UCPD's Article 3 (4) includes built-in provisions to ensure that there are no conflicts between the rules applicable in the UCPD and other EU rules, including sectoral rules relating to unfair practices. This makes clear that "*In the case of conflict between the provisions of this Directive and other Community rules regulating specific aspects of unfair commercial practices, the latter shall prevail and apply to those specific aspects.*" In other EU laws, the prevailing rule may not be made explicit in reverse. For instance, in the (proposed) AI Act, it is stated that all rights and remedies provided for Union law to consumer "remained unaffected and are applicable." The wording is clear enough here to ensure that the level of consumer protection is preserved, but that is not entailing necessarily full coherence if the exercise of such remedies might require certain adaptations.
- The Guidance notes that "the more specific requirements laid down under other EU rules usually add to the general requirements set out in the UCPD. Typically, the UCPD can be used to prevent traders from providing the information required by the sector specific legislation in a misleading or aggressive manner, unless this aspect is specifically regulated by the sector-specific rules."

However, and on some of the basis noted above, this does not necessarily mean all stakeholders regard the legal framework as fully coherent, as is clear from the stakeholder feedback on external coherence questions in the public consultation and targeted surveys.

A distinction needs to be made between a purely legalistic assessment, and perceptions of coherence among stakeholders as to whether the legal framework is clear and understandable also matters. Some stakeholders have observed across various consultations that some issues are covered in multiple pieces of EU legislation but from different perspectives, such as dark patterns and influencer marketing (see next section). This

³⁹⁷ The *lex specialis* principle means that more general rules under the UCPD does not negate the need for platforms to comply with the more specific rules applicable on dark patterns under the DSA. Nonetheless, legal academics have raised a strategic question about how far having different rules in consumer and digital law on dark patterns is able to deliver regulatory clarity and certainty to traders and consumers.

was backed up by evidence from interviews and in responses to the targeted consultation. For example, in an open targeted response, a national Ministry in Austria commented that:

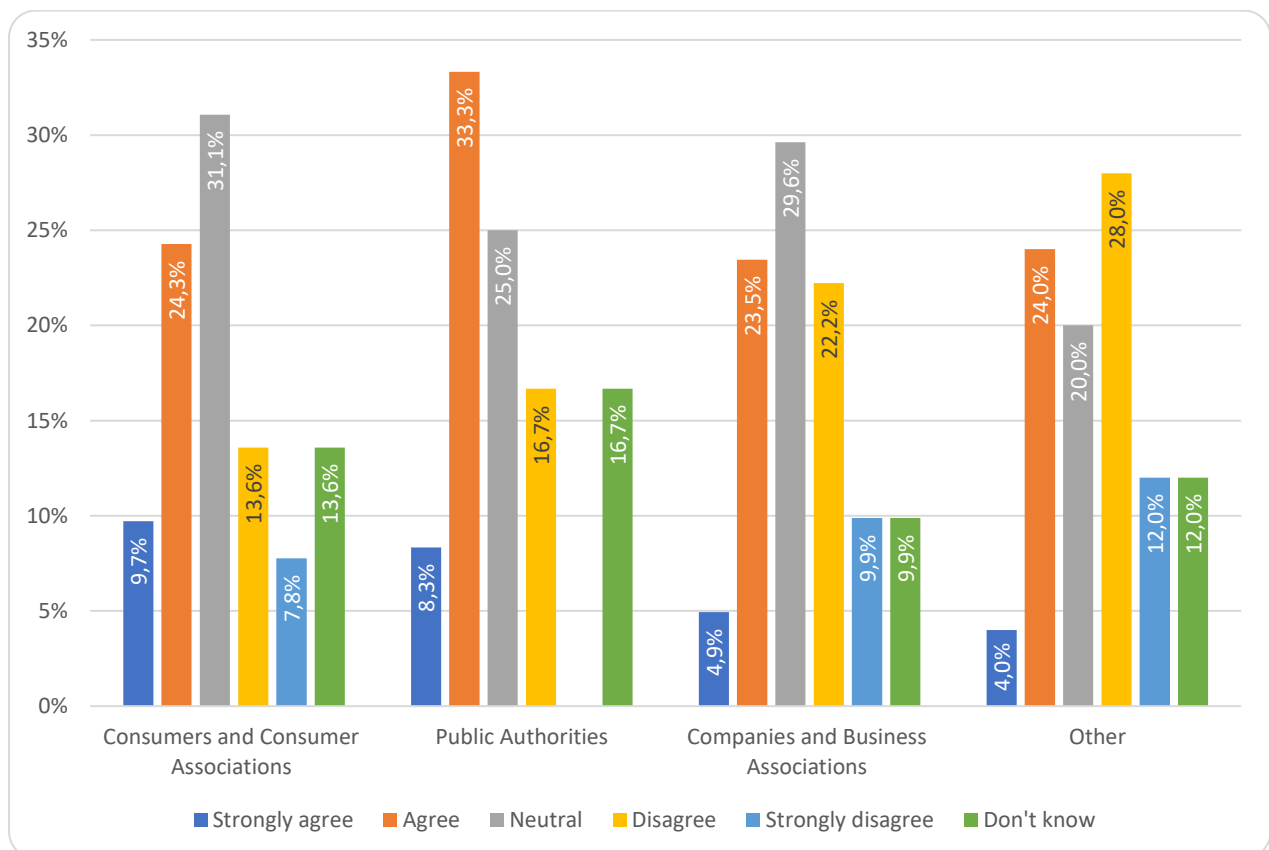
“Just because regulations are not incoherent and thus apply in parallel, this still means a burden for legal practitioners because a multitude of legal acts (EU regulations, national law) have to be examined in order to comply with all provisions. For example, the DSA, UCPD, AVMSD and Directive 2000/31/EC all contain provisions on transparency in advertising, which is burdensome. In order to avoid incoherence, the coherence with existing EU law should be examined in more detail in Impact Assessments and in the legal act itself (the general provision “without prejudice to..” does not provide legal certainty in many cases).”

The perception of coherence by stakeholders is also relevant as it enhances legal certainty and has the potential to reduce (or at least avoid additional) compliance costs. Lack of coherence may be perceived in areas where various pieces of legislation apply, with different goals, sometimes disparate terminology, or diverse level of detail.

Survey findings on coherence

Perceptions of coherence between EU consumer law and other EU legislation were solicited from stakeholders through the public consultation and targeted consultation. Whereas in the former, the focus was on general perceptions of coherence, in the targeted, the questions asked were more technical asking for feedback on coherence between EU consumer law and other individual pieces of law, digital, data-related and other.

Figure 3.33 – To what extent do you agree/ disagree with the following statements? The existing EU consumer laws are coherent with other laws, such as on data protection, new rules applicable to online platforms, artificial intelligence etc. (n = 221)

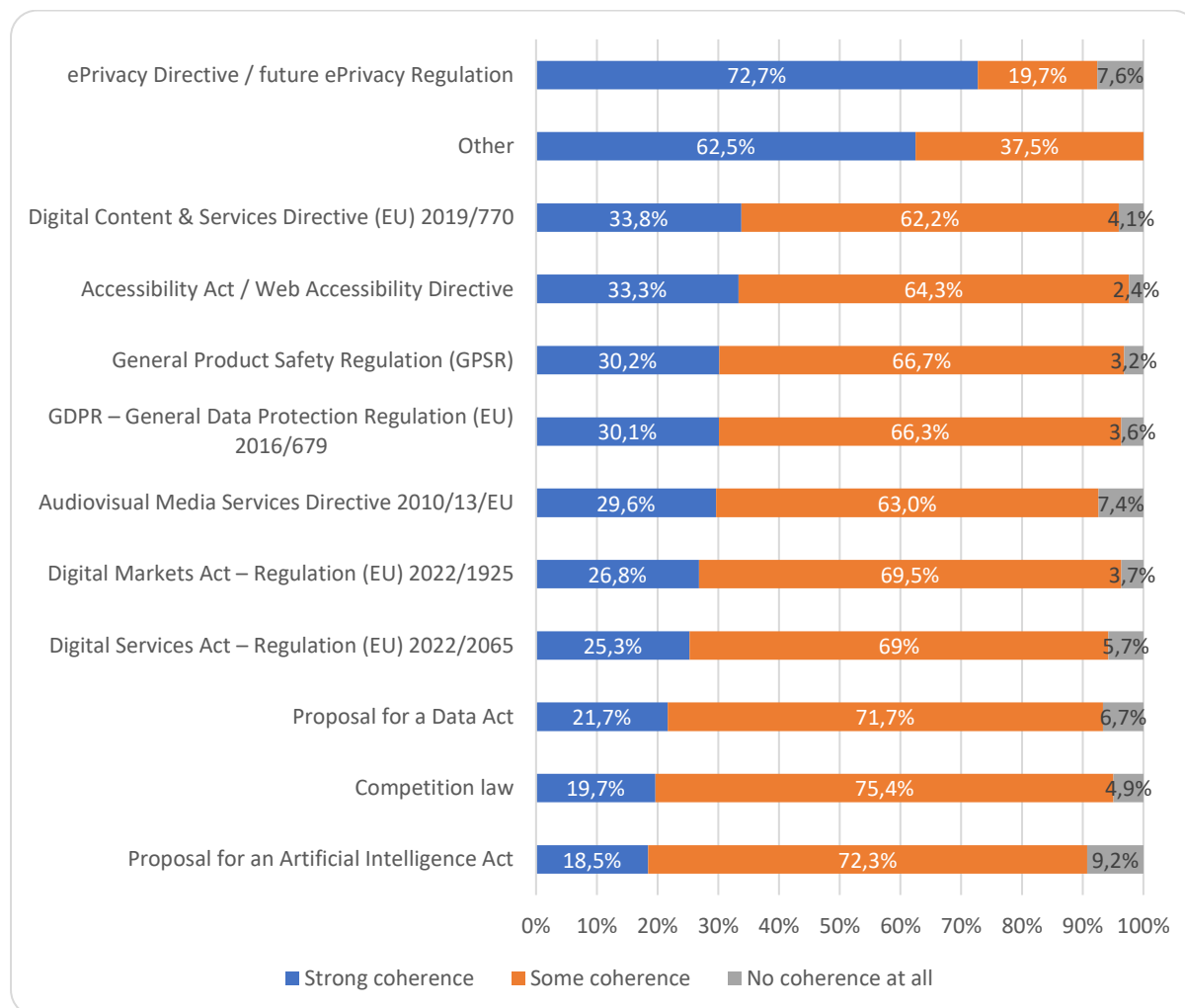


Source: *public consultation survey*

In the **public consultation survey**, respondents were asked about whether existing EU consumer laws are coherent with other laws, such as on data protection, new rules applicable to online platforms, AI etc. The responses are shown disaggregated by stakeholder type.

- Among **consumers and consumer associations**, 34.0% agreed (9.7% strongly agreed and 24.3% agreed), 25.0% were neutral, 13.6% disagreed and 7.8% disagreed strongly and 13.6% stated they did not know.
- Among **public authorities**, 41.6% agreed (8.3% strongly agreed and 33.3% agreed), 31.1% were neutral, and 16.7% disagreed whereas no respondents disagreed strongly. A further 16.7% stated 'don't know.'
- Among **trader associations and individual enterprises**, 28.4% agreed (4.9% strongly agreed and 23.5% agreed), 20.0% were neutral, 22.2% disagreed and a further 9.9% disagreed strongly and 9.9% said "don't know."
- Among **other types of stakeholders**, such as legal academics and NGOs, trade unions etc. 28.0% agreed (only 4.0% strongly agreed and 24.0% agreed), 25.0% were neutral, 28.0% disagreed and 12.0% disagreed strongly. 12.0% said they do not know.
- In the **targeted consultation**, stakeholders were asked whether they perceived EU consumer law to be coherent with other types of EU legislation.

Figure 3.34 – Coherence between EU consumer law and other EU legislation



Source: targeted consultation

Most stakeholders perceived there to be either ‘strong coherence’ or ‘some coherence’ between EU consumer law and other relevant pieces of EU law, including digital laws, data laws, and other types of laws, such as audiovisual media services, web accessibility and competition law. Only a small proportion of respondents expressed the view that there was no coherence at all e.g. 9.2% in the case of the AI Act, 7.6% for the e-Privacy Directive and Proposal for an e-Privacy Regulation, and 7.4% in the case of the Audiovisual Media Services Directive (AVMSD). Regarding the findings, it is interesting that there are considerable variations across different Directives:

The e-PD is perceived as having strongest coherence with the EU consumer law framework. This could reflect the fact it was adopted in 2002, and therefore its provisions were considered when the UCPD and CRD were drawn up to avoid incoherence.

To interpret the variations in responses between Directives, it is necessary to consider both any open targeted survey feedback as well as interview feedback. Later in this section, after presenting the public consultation findings below on coherence, we therefore consider stakeholder feedback in more detail.

It should be noted here how the “strong coherence” perception declined significantly and increasingly in relation to those digital laws that, as it has been stressed above, are neither “launched” nor “perceived” as consumer protection laws, even if they are presented as

complementary with the consumer legislation and promoting consumers' interests (namely, AI Act, Data Act, DSA, DMA).

External coherence – digital laws

In the past five years, reflecting rapid developments in digital markets and services, a series of new EU laws have been adopted in relation to regulating the digital environment and strengthening consumer protection from a sectoral and horizontal perspective. For instance, 2022 introduced the Digital Services Act and Digital Markets Act which aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. Digital laws have sought to address regulatory gaps and to provide consumers with additional protection wherever there are market failures, enhance transparency, and fairness, or promote policy goals that embed consumers' interests such as safety, human rights, rule of law, or a human centric AI development. These perspectives must be considered as explain the different layers where coherence is to be assessed and why the intensity of the interplay between consumer laws and other EU laws is in these cases either less visible or simply lower.

More generally, there is increasing interconnectedness in the context of the European digital economy between EU consumer law, data, and digital laws, raising issues around the challenges to ensure adequate coherence across the *EU acquis* in these areas in the context of the data economy. Whilst these different areas of law have been grouped together under different sub-sections, digital and data laws are closely inter-connected, and there are also challenges around how best to update consumer law for the digital age. A further consideration is that whilst some issues relating to new technologies and digital business practices have already been regulated, there are emerging areas where regulatory certainty is lacking.

For instance, despite the global first of adopting a comprehensive regulation on AI in the AI Act, there are new areas such as the rapid development of generative AI that may raise new regulatory issues which are being monitored. There is then the challenge as to whether to leave these more specific provisions in digital laws only, or to mirror or adapt some of them to EU consumer law. The use of AI in and for contracting (automated decision making throughout the contract life cycle) is another illustrative area. While general principles and rules of contract law may be largely still in national laws, the Union will have to assess the readiness of EU consumer laws to provide adequate protection in new digital contexts, for instance automated and algorithmic contracts.

External coherence – data laws

Privacy is a widely recognised fundamental human right and is broader than data protection, which covers all personal data regardless of the impact on privacy.³⁹⁸ Art. 8(2) of the Charter of Fundamental Rights contains key data protection principles (fair processing, consent or legitimate aim prescribed by law, right to access and rectification). Art. 8(3) of the Charter requires that compliance with data protection rules be subject to control by an independent authority, the EDPB. This is relevant to the application of EU consumer law, for instance, as consent is required to be able to collection and process consumers' personal data, otherwise this could be considered as unfair or deceptive if consumers are not informed that their data is being collected and processed for commercial purposes.

Consumers face persistent and deep-seated privacy challenges in the digital age compared with offline transactions, therefore protecting consumers' personal data and privacy both offline and online should be an integral part of EU consumer protection law in the digital age.

³⁹⁸ Protecting consumer's data in the digital world: Advocating Fairness by Design, Prof. Christine Riefa, University of Reading, School of Law
https://unctad.org/system/files/non-official-document/ccpb_Speaking_Notes_Riefa_digital_data_protection_en.pdf

However, consumer law and data protection law have evolved separately in different ways and this has posed challenges in terms of their coherence and inter-relationship. A 2017 research paper by Helberger, Zuiderveen and Reyna observed that:

“For a long time, consumer law and data protection law belonged to two different worlds. Consumer law is primarily concerned with consumers and their relations with traders of products and services. Consumer law confers mandatory rights on consumers, to create a fair legal playing field for economic transactions. Data protection law aims to protect fairness and fundamental rights when personal data are processed. Consumer law deals with fair contracting; data protection law with fair processing.”³⁹⁹

However, in the digital economy, the consumer protection and data protection legal frameworks need to come together in a way that ensures effective consumer data protection. For instance, online digital services are often paid for in exchange for personal data. The collection of data is also critical for many “smart” consumer products and services which are data-driven in the context of the Internet of Things (IoT).

The above 2017 research paper notes that *“there is growing criticism that data protection law alone, with its strong focus on informed consent as a legal basis for data processing in consumer transactions, may not always provide optimal protection of the interests of digital consumers”*. The authors argue that there are different approaches to dealing with the legal aspects of the more significant role of personal data in consumer markets, either a strict division between the roles of consumer law and data protection law respectively or to *“accept that the relevant legal framework in data-driven consumer markets is not a matter of either data protection law or consumer law”*, but that, instead, data protection law and consumer law could apply in parallel, and could ideally complement each other and offer a sufficiently diverse toolbox of rights and remedies to provide a high level of protection of consumers in digital markets.

Irrespective of precisely how personal data is regulated in consumer markets, strong coherence is needed between EU consumer law and EU data laws as personal data has become increasingly important in the context of the Digital Single Market (DSM) as data collection and processing alongside big data analytics are a crucial element of many commercial practices in today’s data-driven digital economy. The UCPD is especially relevant in this regard given it secures the fairness of commercial practices in business-to-consumer relationships. Compared with a decade ago, EU data protection laws have been introduced that considerably enhance the legal framework, developments which have had implications for EU consumer law as the two different types of law need to be applied in parallel.

Inter-relationship between EU consumer law and other relevant legislation

The inter-relationship between EU consumer law and other relevant legislation is now analysed. For each piece of law, an introductory table is provided highlighting links with EU consumer law. Examples of any legal issues raised relating to coherence are then provided, together with an assessment of stakeholder feedback regarding perceptions of coherence.

As noted earlier, the targeted survey asked for Directive-specific perceptions about coherence. The findings are therefore presented in this section, and complemented by detailed findings based on interview feedback and desk research.

3.5.2 Digital Services Act

The DSA aims to contribute to the proper functioning of the internal market for intermediary

³⁹⁹ Frederik Zuiderveen Borgesius, Natali Helberger, Agustin Reyna, 'The perfect match? A closer look at the relationship between EU consumer law and data protection law', (2017), 54, Common Market Law Review, Issue 5, pp. 1427-1465, <https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/54.5/COLA2017118>

services by providing for a harmonised legal framework that facilitates innovation and ensure the effective protection of fundamental rights, including the principle of consumer protection. Unlike the ECD whose transposition in the national legal systems of the Member States allowed a margin of inharmony, the DSA provides for harmonised rules by way of a Regulation. Beyond the basic provisions of the ECD regulating information society services and intermediary services, the DSA contains a significantly broader and more complete set of rules. First, while the liability exemption is preserved, there are innovations (jurisprudential interpretation of the active role of intermediaries or Art. 6(3) DSA). Second, under a staggered scheme, the DSA set out specific due diligence obligations for certain categories of intermediary services providers (including online platforms and very large online platforms). Third, the DSA includes a detailed and elaborate enforcement system.

So, while DSA is concerned with regulating intermediary service providers, EU consumer law has traditionally focused on the relationship between consumers and traders. Nonetheless, the principle of consumer protection is explicitly acknowledged as one of the goals of the Regulation (Art.1.1 DSA), and by protecting the “recipient of the service” with a number of legal rules, consumers’ interests are also observed. In the staggered model for the application of due diligence obligations, Section 4 adds in fact additional provisions applicable to “providers of online platforms allowing consumers to conclude distance contracts with traders”. It addresses transparency in advertising and prohibits the targeting of minors as well as targeted advertising using profiling based on the use of sensitive data (e.g. sexual orientation, religious belief, political orientation, ethnicity). Users of platforms have more control over how their personal data are used for online advertising.

The DSA is focused on regulating platforms, mainly large and medium-sized platforms. There are additionally some provisions that are only applicable to Very Large Online Platforms (VLOPs), and Very Large Online Search Engines (VLOSEs), as per the tabular overview available in the following online mapping.⁴⁰⁰ Furthermore, several provisions of the DSA shall not apply to online platforms that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC.

Regarding the implications for EU consumer law, the fact that some rules are only applicable to VLOPs and VLOSEs raises a question as to whether if some of the DSA’s rules were to be replicated and/ or customised for EU consumer law generally and therefore made applicable to a wider range of traders how administratively burdensome this may be and how much compliance costs may increase with impact on disputability of markets and competition of smaller platforms. This would likely vary according to the specific legal provisions concerned. For instance, extending the prohibition in the use of sensitive data for profiling purposes is already a legal requirement in the GDPR (and DSA) so its extension to the UCPD would not be a new requirement, but a legal tidying up exercise to improve coherence.

Several stakeholders interviewed (e.g. legal academics, Ministries, consumer ombudsmen) referred to challenges about the lack of perceived coherence and alignment between the DSA and the UCPD.

EU legislation	Introduction and linkage with EU consumer law
<p>Digital Services Act (DSA)</p>	<ul style="list-style-type: none"> • The DSA came into force on 16 November 2022 and started applying from January 1st, 2024⁴⁰¹ (February 17th for platforms publishing their active users). • The DSA is without prejudice to Union law on consumer protection, including

⁴⁰⁰ The Commission designated VLOPs and VLOSEs in 2023 based on criteria laid out in the DSA and a threshold number of 45 million monthly users across the EU. The DSA obligations for these designated online platforms became applicable on August 25, 2023. <https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/>

⁴⁰¹⁴⁰¹ <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

EU legislation	Introduction and linkage with EU consumer law
	<p>the UCPD, CRD and UCTD (Recital 10, DSA).</p> <ul style="list-style-type: none"> • The DSA is relevant to EU consumer law in several ways. It provides additional consumer protection by regulating online marketplaces, online advertising and requiring greater transparency in terms and conditions of service providers, and a clear framework for content moderation (notice and action mechanisms, statement of reasons, transparency of terms of use, etc). • It also regulates certain business practices more explicitly compared with the UCPD, such as dark patterns. The DSA also addresses the issue of dark patterns deployed by platforms but also in the context of intermediation services.

The most relevant Articles in the DSA from an EU consumer law perspective are now summarised. Issues regarding the interplay between the DSA and EU consumer law are then analysed.

Article 25 Dark patterns

Dark patterns are defined as online interface design elements that either deceive, manipulate, or otherwise materially distort/impair the users' ability to make free and informed decisions.⁴⁰²

- Paragraph 2 of Article 25 explicitly addresses the interplay with UCPD and Regulation 2016/679 with a "non-application" rule. Art. 25 applies only to online platforms, while UCPD applies to traders.

To the extent that providers of online platforms are traders, both instruments concurrently apply in some cases under the rule of Art. 25 (2) ("prohibition shall not apply"). Art. 25 DSA refers to any recipient of the service, which includes consumers. However, there is not the benchmark of the "average consumer" which is present in the UCPD and UCTD.

- Art. 25 DSA wording seems to exclusively cover "online interfaces" while dark patterns can take other forms as unfair practices and in that regard be covered by UCPD under the general clauses or under any of the listed practices.

Regarding feedback on coherence, Art. 25(1) was viewed as establishing a clear relationship between the DSA and other applicable legislation, notably the UCPD, given that *lex specialis* is applicable. However, Art 25(2) was viewed as being contradictory and making it difficult to understand the relationship between the UCPD and DSA. It is not evident what means that the "prohibition does not apply" where the UCPD applies. It seems to entail a total distinction of the two regimes but practices can be concurrently covered by both instruments and then Art. 25(2) DSA does not solve the overlap. Many stakeholders (e.g. legal academics, Ministries, CPAs) were of the view that this provision should be clarified.

Traders and their representative associations interviewed mentioned that despite progress made through the DSA in defining dark patterns, it remains difficult to define these more precisely. There was a concern among industry that the concept has gradually been broadened over time. Some studies were seen as having defined dark patterns in a broad sense, making rules prohibiting such practices in the UCPD more difficult to be applied. A legal academic contributing to the study also raised the issue that it could be problematic to introduce a detailed definition of dark patterns in the UCPD, as the concept itself is constantly evolving outside of EU, as codified in the development of different taxonomies. They suggested instead that dark patterns should be an umbrella term to cover unfair commercial practices in the digital environment. However, if the concepts of misleading and aggressive

⁴⁰² Examples of such interface design elements are mentioned in Recital 67. These include exploitative design choices, repeatedly requesting a recipient of a service to make a choice, and making the procedure of cancelling a service significantly more cumbersome than signing up.

commercial practices are applied to dark patterns, there is a risk that everything could be considered a dark pattern.

Due to perceived high levels of non-compliance among traders with existing general provisions in the UCPD that prohibit dark patterns, the rules should be made more explicit in the UCPD rather than only in the guidance, to ensure the legal framework is consistent overall with the DSA, which is only applicable to platforms. However, some stakeholders (mainly trader associations and traders) stated that the problem with dark patterns is down to poor enforcement.

Whilst the DSA describes certain online interface design and prohibits certain forms of dark patterns, these may be deployed in other digital contexts and not only by platforms. The UCPD and GDPR rules as these pieces of law take precedence over the DSA. Some legal academics interviewed commented that it is unclear the circumstances in which a platform should follow the more specific UCPD rules on dark patterns, as opposed to the DSA's Art. 25 and Art. 31.

Article 27 - Recommender system transparency. Consumers will be able to choose recommendation systems based on clear and intelligible explanation of the parameters used, the operation of the systems and the reasons why certain options are recommended. Recommender systems determine the content that users see and offers they receive in the digital environments. They are a tool to structure large amounts of information to provide users with (potentially) relevant information, which in turn influences decision-making. They determine the “visibility” of traders and products or offers, and consequently, the likeliness to have impact on the market. Consequently, unlike search system that provide (under certain criteria) a list of result, the “recommending” role of recommender systems aims and is more likely to impact on the final decision of the recipient of the service. Therefore, awareness and control by the recipient of the service over the main parameters and the reasons for the relative importance/weight are provided for by Art. 27 DSA. In some circumstances, moreover, recommender systems can be manipulative and permeate dark practices. According to some literature, for instance, *“recommender systems present risks for consumer autonomy, especially in terms of privacy, independence and reciprocity”*.⁴⁰³ Accordingly, the DSA has regulated the transparency of recommender systems. Transparency requirements relate to understanding the criteria and where possible, to change the preferred options.

- **Art. 27(1).** Providers of online platforms that use recommender systems shall set out in their terms and conditions, in **plain and intelligible language, the main parameters used in their recommender systems**, as well as any options for the recipients of the service to modify or influence those main parameters.
- **Art. 27(2).** The main parameters referred to in para 1 shall **explain why certain information is suggested to the recipient of the service**. They shall include, at least: (a) the criteria which are most significant in determining the information suggested to the recipient of the service; and (b) the reasons for the relative importance of those parameters.
- **Art. 27(3).** Where several options are available for recommender systems that determine the **relative order of information presented to recipients of the service**, providers of online platforms shall also make available a functionality that allows the recipient of the service to select and to modify at any time their preferred option. Art. 27(3) DSA refers to rendering it easier by providing direct access to the required functionality in the online interface. So indirectly, it is expected that the online interface

⁴⁰³ Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A Long-Term Approach. Published online by Cambridge University Press: 03 August 2023, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/preserving-consumer-autonomy-through-european-union-regulation-of-artificial-intelligence-a-longterm-approach/C59490014B968AB10ECA772683D2B283>

is not designed in a way that renders uneasy or costly to access the functionality.

Art. 27 on recommender systems is concerned with a series of provisions to strengthen transparency. A parallel can be drawn with the changes made through the MD to regulate platforms to provide **transparency in search rankings**.

In addition to the requirements set out in Article 27, Article 38 states that providers of very large online platforms and of very large online search engines that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of the GDPR.

- Whereas measures under the DSA allow consumers to **opt out of personalisation through recommender systems**, this is not presently the case under the UCPD which does not explicitly regulate recommender systems, although should such systems amount to be an unfair practice, they are presently indirectly covered through the general clauses of the UCPD.
- The interplay with Art. 22 GDPR referring to the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the affected person. While recommender systems used in the context of commercial transactions to help consumers to decide which product to buy and with which trade to deal, profiling-based recommender systems in other contexts may lead to a concurrent application if the systems limit the access of a person to a certain service based on the profiling, or the recommender system is directed to assess eligibility, for instance.

Article 34 - risk assessments

The DSA's requirement for VLOPs and VLOSEs to submit risk assessments and risk mitigation measures could capture a very broad range of consumer protection issues. Article 34 provides that the providers shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. The risk assessments shall be done at least once every year and in any event before deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include systemic risks, among others, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high level of consumer protection enshrined in Article 38 of the Charter.

In this regard, in the risk assessment, very large online platforms should assess whether the design and operation of their algorithmic systems, including recommender systems, have any actual or foreseeable impact on the level of consumer protection.

Articles 26 and 39 - Online advertising and the restrictions to targeted advertising

Articles 26 and 39 address different aspects of online advertising, including the importance of transparency to make clear that adverts are labelled as such. Art. 26 is in the section devoted to all online platforms, while Art. 39 applies to very large online platforms.

Art. 26, Subject matter

1. Providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time, the following:

- (a) that the information is an advertisement, including through prominent markings, which might follow standards pursuant to Article 44;

- (b) the natural or legal person on whose behalf the advertisement is presented;
- (c) the natural or legal person who paid for the advertisement if that person is different from the natural or legal person referred to in point (b);
- (d) meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters.

2. Providers of online platforms shall provide recipients of the service with a functionality to declare whether the content they provide is or contains commercial communications.

The DSA sets out more detailed rules regarding transparency in advertising for online platforms compared with the UCPD, which whilst having prohibited hidden advertising does not set out any specific detailed rules on transparency requirements. Interestingly, the DSA provides for the obligation of online platforms to provide a functionality for any recipient of the service to declare that the content they post or provide is or contain commercial communication. So, the due diligence obligation is placed on the platform and consists of a duty to provide a functionality and ensure that other recipients of the service can identify it as such.

Article 26(3) - Providers of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679.

The DSA prohibits targeted advertising based on the profiling of sensitive data within the meaning of Article 9(1), GDPR. It is therefore no longer possible for platforms to display adverts based on a person's sensitive data. In the UCPD, there is no explicit prohibition of the use of sensitive data in profiling for personalised advertising purposes.

Article 28 - Online protection of minors

The protection of minors is covered in the DSA under Article 28(1) and (2), as well as in Art. 34(1)(d) relating to risk assessment.

- Art. 28(1) - Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service.
- Art. 28(2) – Providers of online platforms shall not present advertisements on their interface based on profiling.

Under the DSA, it is no longer possible for platforms to display adverts based on profiling using children's personal data. The UCPD itself sets a special level of protection for children as they have been explicitly listed as one of the types of vulnerable consumers that deserve additional level of protection due to their age which leads to the presence of their vulnerability in the decision-making process leading to transactional decisions in the digital environment. The UCPD sets the benchmark of the "average" member of the group of consumers particularly vulnerable because of age or credulity to assess the commercial practices. The DSA refer to minors and require "appropriateness and proportionality" in the measures to ensure a high level of privacy, safety, and security. Wording and terminology differ, although intended meanings are not elusive. Moreover, minors are not explicitly protected from targeted advertising using profiling practices which can be common in the digital environment, although they are protected through the more general provisions on the use of sensitive personal data under Art. 9 GDPR). This issue – as with sensitive data - is considered in more detail in the thematic assessment of the interaction between EU data and consumer laws (see Section 3.7).

The risk assessments in Art. 34(1)(d) cover any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and **minors and serious negative consequences to the person's physical and mental well-being**.

The requirement to carry out risk assessment in relation to the protection of minors and other vulnerable groups, including in respect of people's physical and mental well-being is especially relevant to online platforms, given issues regarding high-profile cases when people's mental well-being has been affected by algorithmic-driven content, for instance in relation to self-harm. This does however raise the issue that as Art. 5(3) provides additional protection for vulnerable consumers, whether there is a need to mirror the DSA by ensuring that protection of minors and attention to people's physical and mental well-being is extended for the digital age to all relevant traders. The DSA provides for an active and positive obligation to the high level of protection and on an adequate and proportionate basis; whereas the UCPD draws a red line (more intensely because of the age-based vulnerability) on those commercial practices which are likely to materially distort the economic behaviour of such a group of consumers. There is no incoherence, but goals and measures, albeit being complementary, are not aligned. Online platforms raise issues concerning digital addiction that may lead to mental health problems, but also other digital products, such as video games. Risk assessment in the context of EU consumer law could be considered to ensure that such negative effects are fully considered by platforms when designing services.

Lastly, in respect of minor protection, the **DSA's Art. 44(1)(j) standards includes targeted measures to protect minors online**.

Article 30 - Traceability of traders

The DSA mandates transparency requirements for platforms to ensure that traders are identified/identifiable. It is one of the additional provisions applicable to online platforms allowing consumers to conclude distance contracts with traders. Whilst some of the information required relates to information provision to be retained by the platform in case of request by a CPA, other information must be made available on the platform. The aim of this provision is not enhancing the information on traders to be provided to consumers. The aim is to ensure that traders are traceable and can be traced, preventing false accounts, anonymous (untraceable) transactions, or misleading traders' details. That is why, as per Art. 30(7) only the items under points a, d and e (contact details, registration, self-certification) of paragraph 1 of the same article to be made available to the recipients of the service.

Under Art. 30(7), the provider of the online platform allowing consumers to conclude distance contracts with traders shall make the information referred to in paragraph 1, points (a), (d) and (e) available on its online platform to the recipients of the service in a clear, easily accessible and comprehensible manner. That information shall be available at least on the online platform's online interface where the information on the product or service is presented.

- Art. 30(1)(a) the name, address, telephone number and email address of the trader;
- Art. 30(d) where the trader is registered in a trade register or similar public register, the trade register in which the trader is registered and its registration number or equivalent means of identification in that register;
- Art. 30 (e) a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.

Article 30 DSA is complementary to strengthening transparency through the Modernisation Directive, which requires the status of sellers using their platforms to be indicated to allow consumers to know whether they are entering a contract with a professional trader or a private individual. This was viewed to be complementary and not duplicative by stakeholders consulted. There is no contradiction nor overlap, but complementariness within their respective scopes of applications.

This raises issues however regarding what types of information should be provided about the trader to consumers under the CRD for contracts other than those conducted through online platforms falling under the DSA. **Article 6(1) of the CRD ‘Information requirements for distance and off-premises contracts’** requires the geographical address at which the trader is established and the trader’s telephone number, fax number and email address, where available, to enable the consumer to contact the trader quickly and communicate with him efficiently. However, it does not presently include a requirement to provide traders details on a trade register or self-certification that the trader complies with all applicable EU laws.

Further transparency could help consumers to verify who the trader is before they conclude a transaction. More detailed information would also be required by consumers when things go wrong and they wish to make a complaint and cannot get hold of the trader by other means. It could be argued that the focus in both the CRD and the DSA leaves an omission in terms of communication means as many traders and consumers prefer to interact in the digital environment via chatbots directly in-app and/ or via a website interface design to resolve complaints and other issues. A reference to communication and interaction means other than phone number and email address in a more technology-neutral way would have been desirable.

Article 31 – Compliance by design (online marketplaces)

Article 31 on compliance by design is relevant to distance contracts, including those falling under the CRD. There is also a link to interface design and therefore to dark patterns. Under Article 31, providers shall ensure that its online interface is designed and organised in a way that enables traders to comply with their obligations regarding pre-contractual information, compliance and product safety information under applicable Union law. Traders should be able to provide at least the following information:

- (a) the information necessary for the clear and unambiguous identification of the products or the services promoted or offered to consumers located in the Union through the services of the providers;
- (b) any sign identifying the trader such as the trademark, symbol or logo; and,
- (c) where applicable, the information concerning the labelling and marking in compliance with rules of applicable Union law on product safety and product compliance.

The DSA places the onus on providers of online platforms allowing consumers to conclude distance contracts with traders to check themselves whether traders have provided the necessary information referred to in paragraphs 1 and 2 above prior to allowing them to offer their products or services on those platforms. The CRD does not currently include any compliance by design type requirements to ensure that pre-contractual information is provided clearly on different interfaces e.g. apps, websites etc. However, there are medium-sensitive requirements referring “to the extent appropriate to the medium” (Art. 6 CRD). Pre-contractual information should be easily readable and understandable by an average consumer and should be provided in a clear, legible, and comprehensible manner. In fact, the CRD already refers to the need for such information to be clear and intelligible. Article 5 provides the list of pre-contractual information that should be provided for in-shop purchases and Article 6 lists the information requirements for distance and off-premise contracts (e.g. online purchases), including the existence of a right of withdrawal.

DSA and CRD obligations are directly addressed to different parties. While DSA compliance by design obligations are imposed on platform operators, CRD obligations are directly allocated on the trader vis-à-vis the consumer. Although based on personal scope, there is *per se* incoherence, an alignment in this case turns out to be particularly pressing and expected, as Art. 31 contains one of the additional obligations applicable to providers of online platform allowing consumers to conclude distance contracts with traders. Alignment is not necessarily bidirectional. On the one hand, the compliance by design obligation is feasible where distance contracts take place in a platform or similar digital environments designed and/or operated by the trader or by a third party, but it is not, at least strictly, applicable on other off-premises and distance contracts as defined by the CRD (Art. 2 CRD). On the other hand, however, it is justified that the items of information whose provision by the trader the online interface is going to facilitate as per Art. 31 DSA do differ.

These provisions would be better aligned with the DSA and clearer if not only did information have to be clear and intelligible, but also presented in a way that avoids dark patterns in interface design such as to avoid such information being difficult to find. Whilst arguably it made sense to regulate platforms first regarding compliance by design requirements to ensure pre-contractual information is clear and easily available to the average consumer, there would be strong rationale in extending this requirement to include all digital interfaces irrespective of the type of trader. This would be a means of strengthening prohibition of dark patterns, which are already prohibited in theory but without any detailed provisions.

Article 44 - Standards to be developed for interface design

Given the importance of ensuring fairness in interface design addressed in Art. 31 (compliance by design) to facilitate the application of compliance by design principles and as noted earlier the protection of minors, the DSA includes provisions on standards. Specifically, Art. 44(1)(b) (h) (i) (j) pertain to standards relevant in the B2C context. These relevant provisions are highlighted below.

Art. 44(1). The Commission shall consult the Board, and shall support and promote the development and implementation of voluntary standards set by relevant European and international standardisation bodies, at least in respect of the following:

- (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 relating to advertising contained in this Regulation, including the obligations regarding prominent markings for advertisements and commercial communications referred to in Article 26;
- (i) choice interfaces and presentation of information on the main parameters of different types of recommender systems, in accordance with Articles 27 and 38;
- (j) standards for targeted measures to protect minors online.

Art. 44(2). The Commission shall support the update of the standards in the light of technological developments [.....].

Several legal academics stressed that voluntary standards could potentially play an important role both in interviews and in some of the consultation responses. However, others expressed the view that experience shows the effectiveness of this instrument is limited as traders may perceive standards as being overly prescriptive in terms of digital design interfaces, for example. Given the growing importance of promoting good practice in design interfaces and minimising negative impacts such as those stemming from digital addiction, it may be discussed whether standards could also play a key role in the UCPD. The role of standards, as stressed in the DSA, was raised by some stakeholders as being relevant in fostering digital fairness by design from the outset. However, traders and their associations were concerned that voluntary standards could become mandatory in future and this could risk being overly prescriptive and insufficiently technology-neutral. An example was in relation to the possibility of rules relating to the design of withdrawal and cancellation buttons. Different technical

solutions would be needed for different interfaces, therefore trader associations and traders recommended only setting general parameters and not detailed design requirements. Hence, the role of standards can also be relevant in relation to formal requirements in distance contracts by electronic means under the CRD or, as mentioned, in implementing withdrawal and cancellation buttons.

3.5.3 Digital Markets Act

EU legislation	Introduction and linkage with EU consumer law
<p>Digital Markets Act (DMA)</p>	<ul style="list-style-type: none"> • The DMA came into force in 2022 and became applicable as of 2 May 2023. Designated gatekeepers were given 6 months (following their designation of 5 September 2023) to comply with the DMA's requirements, at the latest by 6 March 2024. • The DMA's objective is to ensure a safe, fair, and contestable digital market. It seeks to improve fairness and competitiveness in the Digital Single Market by establishing more specific rules for gatekeepers. • The Act is an industry-specific, ex ante regulation with several strict prohibitions and obligations on digital gatekeepers offering core platform services • The DMA takes as a starting point (see Recitals 2 and 13) the fact that unfair practices in the digital sector are particularly common in core platform services due to certain features, including scale economies, strong network effects, an ability to connect many business users with many end-users through the multi-dimensional nature of the services, lock-in effects, a lack of multi-homing, data-driven advantages, and vertical integration. • The DMA improves consumers' rights <i>inter alia</i> by; providing consumers with freedom of choice when selecting and using digital core platform services, increasing interoperability between different platform services, and facilitating data portability and data transfer, ensuring easy uninstallation, making it easier to cancel subscriptions, and eliminating unfair market practices such as self-preferencing, tying, and tracking users without their consent.⁴⁰⁴

The DMA is applicable to systemically-important market players, such as large online-platforms, search engines, cloud services, social networks, video-sharing platforms, online advertising networks, and products and services owned by large digital enterprises. Providers of core platform services with significant impact on the internal market, acting a gateway, and with an entrenched and durable position shall be designated as 'gatekeepers.' Designation is based on the qualitative and quantitative criteria laid down in Art. 3 DMA.⁴⁰⁵

The DMA's policy goals embrace consumer protections but are broader: mitigate serious imbalances in bargaining power and, consequently, unfair practices and conditions for business users, as well as for end users of these services, and, therefore, avoiding the consequential impact on prices, quality, fair competition, and innovation in the digital sector.

The DMA does not explicitly refer to consumers but rather on the concept of end-users. Some legal academics view the DMA as a new Regulation which represents a step in the right direction but is not sufficiently focused on consumer protection in a structurally asymmetric

⁴⁰⁴ Digital Markets Act (DMA): A Consumer Protection Perspective, Anna Moskal, European Forum Highlight published in European Papers - A Journal on Law and Integration, 2022 7(3), 1113-1119.

⁴⁰⁵ In September 2023, the EC designated six gatekeepers: Amazon, Meta, Alphabet, Apple, Microsoft, and ByteDance.

data-driven digital market.

"The DMA is primarily focused on platforms and business users, and it does not acknowledge the role of consumers as a key aspect of market regulation. For instance, consumers/end users were left out of Recital 33, which explains that, for the purpose of the Regulation, "unfairness" should relate to an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage. This definition opts for a bilateral relation rather than a market-based and consumer-oriented approach".⁴⁰⁶

The DMA reinforces the data protection principles set out in the GDPR and e-PD and aims to protect consumers' privacy and prevent unfair practices by digital service providers. Consent management is required to protect core platform services' users' data privacy rights.

Whereas there are several prohibitions for gatekeepers in respect of how they should process personal data, which prevents them combining personal data or using such data from third parties using their platforms, these rules are more relevant to the small number of designated gatekeepers under the DMA. It is questionable whether such provisions would also be necessary under the UCPD, given the market dominance of very large platforms and search engines and their intermediation role, which required separate legislation. Other traders are not in such a strong market position that possible unfair use of personal data presents a risk to the same degree.

- Articles 5 and 6 DMA contain specific prohibitions, with those in Article 5 considered prohibited in all cases, whereas those in Article 6 may be unfair and susceptible to being further specified. Many of these prohibitions are relevant for B2C relationships and a selection will be analysed below.

There are some specific protections for end-users within the DMA in relation to online subscriptions. According to Article 5(8), the gatekeeper shall not require business users or end users to subscribe to, or register with, any further core platform services listed in the designation decision pursuant to Article 3(9) or which meet the thresholds in Article 3(2), point (b), as a condition for being able to use, access, sign up for or registering with any of that gatekeeper's core platform services listed pursuant to that Article. Furthermore, Article 6(13) states that the conditions for terminating core platform services cannot be disproportionate or exercised with undue difficulty.

Recital 63 in relation to subscriptions is also worth mentioning in full here as this explains the principle of being able to exit from subscriptions as being able to enter into them:

"Gatekeepers can hamper the ability of business users and end users to unsubscribe from a core platform service that they have previously subscribed to. Therefore, rules should be established to avoid a situation in which gatekeepers undermine the rights of business users and end users to freely choose which core platform service they use. To safeguard free choice of business users and end users, a gatekeeper should not be allowed to make it unnecessarily difficult or complicated for business users or end users to unsubscribe from a core platform service.

Closing an account or un-subscribing should not be made be more complicated than opening an account or subscribing to the same service. Gatekeepers should not demand additional fees when terminating contracts with their end users or business users. Gatekeepers should ensure that the conditions for terminating contracts are always proportionate and can be exercised without undue difficulty by end users, such as, for example, in relation to the reasons for termination, the notice period, or the form of such termination."

⁴⁰⁶ Digital Markets Act (DMA): A Consumer Protection Perspective, Anna Moskal, European Papers www.europeanpapers.eu ISSN 2499-8249, Vol. 7, 2022, No 3, pp. 1113-1119 DOI: 10.15166/2499-8249/615 (European Forum, 31 January 2022)

The explanation provided in the more detailed preamble is similar to the principle in the UCPD Guidance that in relation to avoiding subscription traps, it should be as easy to enter into a subscription as to exit it. However, the DMA goes further in that there is a legal provision in this regard (no further specification needed as it is laid down in Art. 5 DMA), which could also be considered in future within the UCPD's legal text (but adapting this Article which would not focus on gatekeepers and platform services but simply traders in relation to all subscriptions to prevent subscription traps and avoid consumer detriment due to unnecessary time wasted in cancelling subscriptions. Currently, under the UCPD, these practices would be addressed as UCPD Art. 8 Aggressive practice (coercion), including Art. 9(d) (impose onerous or disproportionate non-contractual barriers where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader) and Art. 7 on misleading omissions.

- Art. 6(4) DMA allowing consumers to easily use third-party software and apps, instead of default software settings for services provided gatekeepers.

The gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper. The gatekeeper shall, where applicable, not prevent the downloaded third-party software applications or software application stores from prompting end users to decide whether they want to set that downloaded software application or software application store as their default. The gatekeeper shall technically enable end users who decide to set that downloaded software application or software application store as their default to carry out that change easily.

Transparency is an important pre-condition to ensure consumer choice. The DMA contains transparency requirements to overcome digital asymmetries in respect of algorithms.

- Art. 6(5) introduced a provision for regulating rankings applications by gatekeepers. The gatekeeper may not favour its products or services over those of third parties in a ranking (Art. 6(5)(1) DMA). The prohibition of self-preference is also extended to indexing and crawling. The ranking must be transparent in general and rankings must be fair and non-discriminatory (Art.6(5)(2) DMA). Article 6(5)(2) DMA distinguishes between transparency, fairness, and non-discrimination. Gatekeepers must give search engine operators access to ranking, search, click and display data of search results on FRAND terms (fair, reasonable and non-discriminatory). However, dedicated sections at the top of a ranking can still be reserved for paid content ("sponsored content"). All rankings, regardless of whether they are sponsored, must be fair and non-discriminatory under the DMA.⁴⁰⁷

The DMA already covers the problem in that the rules are addressed to gatekeepers which is relevant as they control access to app stores and platforms through which consumers access third party software/ apps.

- Art. 6(6) ensures easy switching between, and subscription to, different software applications and services. The gatekeeper shall not restrict technically or otherwise the ability of end users to switch between, and subscribe to, different software applications and services that are accessed using the core platform services of the gatekeeper, including as regards the choice of Internet access services for end users.

⁴⁰⁷ Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and beyond. Authors: Philipp Hacker*, Johann Cordes† and Janina Rochon‡, Working Paper, December 2022 - https://www.researchgate.net/publication/366190644_Regulating_Gatekeeper_AI_and_Data_Transparency_Access_and_Fairness_under_the_DMA_the_GDPR_and_beyond

The UCPD does not mention the need to provide consumers with the right to be able to switch between different software applications and services easily. This issue is not dissimilar to the one mentioned earlier for entering and exiting subscriptions. Consideration could be given to aligning the UCPD with the approach taken in the DMA. However, due consideration would be needed of any contractual law obligations on the consumer e.g. minimum cancellation periods. The problem here is two-fold. On the one hand, when minimum cancellation periods amount to be an unfair practice as rendering in practice switching impossible, too difficult, or highly inconvenient. On the other hand, whether these practices should be extended over any trader or, on the contrary, should only be focused on gatekeepers, as it is in fact their significant impact, and gatekeeping potential what justified the regulatory intervention.

Regarding coherence issues, the transparency of rankings is an important consideration to ensure that consumer choice is not limited and/ or that rankings are unfair and deceptive. Accordingly, **rankings have been addressed in several different pieces of legislation**. In the Consumer Rights Directive (CRD), the focus in the new Art. 6a (as updated by the MD) is on search rankings on online platforms. Unlike Article 6a CRD, Article 7(4a) UCPD is not limited to online marketplaces but applies to all entrepreneurs who enable a search for products of different suppliers. In addition, the issue of transparency in rankings can be covered by the GDPR and the DSA (specifically recommender systems). In addition, ranking has been regulated in the P2B Regulation (only relevant to B2B). The importance of this latter provision (Art. 5 P2B Regulation) is also underlined by the Guidelines on Ranking Transparency published by the European Commission in December 2020.⁴⁰⁸ There do not appear to be any coherence issues as transparency in search rankings have been addressed in several pieces of law, including recently through the MD in EU consumer law.

- Art. 13 DMA on anti-circumvention ensures that gatekeepers do not avoid their obligations under Articles 5, 6 and 7 of the DMA using dark patterns or other means. The DMA prohibits behaviour aimed at subverting or impairing user autonomy, decision-making, or choice, to circumvent the prohibition and obligations that the DMA lays down. This provision avoids that gatekeepers strategically and opportunistically circumvent the application of EU regulations or of the specific obligations under other EU legislation.

Overall, in the stakeholder consultations, there was only limited feedback on the DMA, given that the Regulation is new, the rules are aimed at gatekeepers and largely regulate the relationship between large platforms and other businesses, with consumers indirectly addressed through provisions in relation to end-users.

An EU business association commented in their open targeted response that “*competition instruments such as the DMA, Competition law and the Data Act pursue different objectives compared with consumer protection. As digital markets, especially data-driven marketing, tend to be dominated by few large companies, any decision to update the current consumer protection framework should carefully assess the impact on competition and market functioning which ultimately affect consumers.*” Some legal academics were also of the view that the obligations of gatekeepers should not be extended to all traders, as the objectives of EU rules for gatekeepers are different, as is and the unfairness assessment.

A legal academic interviewed mentioned in relation to the treatment of dark patterns in the DMA and DSA that the provisions on dark patterns should be better coordinated with the UCPD and with the concept of undue influence.

A trader from a large global tech firm stated in the targeted survey that the “DMA prioritises contestability over consumer protection. Depending on interpretation, the DMA could undermine the role of large platforms in protecting users against illegal and harmful practices

⁴⁰⁸ Commission Notice, Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council, 2020 C 424/1, 8.12.2020, p. 1-26.

and lead to consumer confusion over which business they are doing with. It could make it more challenging to enforce the DSA, while increasing risks of user exposure to illegal content. The potential effects of the DMA on consumer protection laws should therefore be closely monitored.”

A business association, the European Tech Alliance (EUTA) noted in relation to the DMA that *“EU competition law and the Data Act are intended to foster competition, while consumer law is increasingly closing access to data, which is paramount for innovation. Recent initiatives and debates around online consumer protection show an intention to base all digital interactions on consent only and to restrain personalisation. At the same time such initiatives are likely to favour actors that already have access to large data sets. This contradiction is very much likely to be detrimental to consumers in the long run, as it will impede EU innovation and reduce alternatives on the digital market.”*

The Dutch consumer protection authority pointed to diverging terminology between different pieces of law. They alluded to different terminology in the DMA i.e. the use of end-users rather than consumers, and in the DSA to recipients of the service that include consumers, and consumers, separately, as well.

3.5.4 AI Act

EU legislation	Introduction and linkage with EU consumer law
<p>Artificial intelligence Act (AIA)</p>	<ul style="list-style-type: none"> • The AI Act was adopted in on 13 June 2024.⁴⁰⁹ • The AIA has adopted a risk-based approach, classifying AI systems into four different risk categories depending on their use. • The AIA protects consumers by regulating high-risk AI systems, and prohibits the use of certain practices and use cases of AI systems that would undermine persons’ rights and/ or create an unacceptable risk. Art. 5 AIA refer to “persons”, whereas the recital expressly mentions consumers. • Under the AI Act, consumers have been given several rights, including a right to be informed when being subject to a decision from a high-risk AI system, a right to complain to an authority about an AI system, the right to bring a supervisory authority to court if it fails to act. Consumers were also given the right to ask for collective redress when an AI system has caused harm to a group of consumers. • Mandatory fundamental rights impact assessments and a right of citizens "to launch complaints about AI systems and receive explanations about decisions based on high-risk AI systems that impact their rights" are also part of the political agreement. • The AIA also regulates the need for transparency to ensure that natural persons interacting with AI systems are informed about that fact and in case they are viewing content that has been AI-generated (e.g. deepfakes).

The specific relevant provisions are now considered. However, as the final legal text has not been published, the analysis is based on the draft proposal.

AIA aims to protect persons’ rights and to ensure a high level of consumer protection. However, its target is broader and the Regulation does not focus on the transactional context

⁴⁰⁹ <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

(trader-consumer) but in a more complex and plural AI supply chain. Consequently, references to consumers are not numerous.

- Art. 5 outlines prohibited AI practices, including the use of AI systems that manipulate human behaviour to circumvent their free will.

This is highly relevant to the UCPD, given the transactional test⁴¹⁰ to assess whether consumers have taken a decision they would not otherwise have taken. The UCPD's general provisions (Articles 5 to 9) cover unfair, misleading, and aggressive commercial practices capable of distorting consumers' economic behaviour, thereby causing or being likely to cause them to take a transactional decision that they would not have taken otherwise. The use of subliminal techniques beyond a person's consciousness³⁷ to manipulate individuals into making decisions that they may not have otherwise made. There are parallels here with the AVMSD's Art. 9(1)(b) which requires that audiovisual commercial communications shall not use subliminal techniques. As in the case of exploitative practices, the AIA is limiting the prohibited practices to those causing or being likely to cause significant harm.

The use of AI to exploit the vulnerabilities of people (due to their age, disability, social or economic situation) to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm. There are links here with the UCPD's Art. 5(3) which provides protection for vulnerable consumers. However, the UCPD is not specific about the fact that the decision taken causes or is likely to cause significant harm to the person affected, another person or a group of persons, whereas the AIA is focused on the specific harm that could be caused by AI. The AIA goes further in terms of the types of vulnerabilities, in that a user's social or economic situation is considered whereas this is not the case in the UCPD, which has a narrower definition of consumer vulnerability (mental or physical infirmity, age or credulity).

High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider.

- Art. 13(3)(b)(iii) provides that any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights.

Given the potential to mislead consumers, some provisions in the AI Act are relevant to the application of EU consumer law. For instance, deep fakes and other AI generated content must be labelled as such through the provision of information to users. Users also need to be informed when biometric categorisation or emotion recognition systems are being used. Biometric categorisation systems that use sensitive characteristics (e.g. political, religious, philosophical beliefs, sexual orientation, race) have also been prohibited.

Presently, the UCPD does not refer to any specific digital practices. However, the transparency requirements in the AIA are relevant as without transparency, the use of certain AI-generated content and of emotion recognition systems could potentially be misleading or deceptive or trick consumers into transactional decisions they would not otherwise have taken.

- Art. 14 stresses the importance of human oversight.

The issue of automation bias is one raised as a concern by BEUC and national consumer protection authorities. Articles 13 and 14 of the AIA are concerned with the risk of users taking

⁴¹⁰ Article 2(k) UCPD provides a definition of the transactional test. A 'transactional decision' means any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting".

decisions they would not otherwise have taken, and therefore there are parallels with the UCPD's general provisions in Art's 5-9. However, the UCPD does not explicitly deal with digitalisation and automation so there is an outstanding coherence issue as to whether the UCPD should explicitly reference the need to strengthen information provision to consumers if there is a risk of bias in AI automation.

The need for regulatory alignment between the AIA and other applicable laws has been factored into the drafting of the legal text. For instance, the AIA makes clear that when harmful AI practices and systems do not fall under the scope of prohibited AI practices as defined in the proposed regulation, they would be covered by general data and consumer protection legislation.

AIA contains obligations at the design and development stages that prevent the risk and mitigate the effects throughout the AI supply chain, and consequently, reinforce the consumer protection at the end-use edge.

There is an emphasis on developers of AI foundation models based on generative AI having to comply with stronger transparency obligations (Art. 52). The latter obligation aims to avoid, through transparency, the use of a generative AI system to create manipulative content. Where a generative AI system has been used to create "deep fakes" (i.e. text, video or audio that appears to be authentic or truthful while it is not), the users that created such content must disclose that the content is AI generated or manipulated and (where possible) indicate the name of the legal or natural person that generated or manipulated the content.⁴¹¹

In terms of stakeholder feedback, some traders were concerned that too much regulation of AI could risk undermining the technology-neutral principle. However, BEUC expressed concerns that the AI Act lacks basic rights for consumers when they are subject to automated decisions made by AI algorithms that could make biased decisions, or interact within an AI system. This raises the issue as to whether such rights should only be included in the AIA, or if such rights could be included in EU consumer more generally.

Some stakeholders have suggested that the Commission should duplicate the two prohibitions in Art. 5(1)(a) and 5(1)(b) in the AI Act (relating to protecting by including these specific practices as prohibited practices in the UCPD Annex). The NCC has raised various additional risks, including the personification of AI models, explicitly invite end users to share information about themselves. For instance, chat applications such as Replika and Snapchat's My AI follow this model, which raises issues around the need to ensure consumer protection among vulnerable consumers, including minors (and to clarify which business purposes – if any – this data can be used for).

In their 2023 report on generative AI⁴¹², the Norwegian Consumer Council (NCC) points to the risks of misleading or unfair commercial practices due to the use of text-based queries compared with conventional search engines from a transparency perspective, and notes the results that come back from prompts may be biased. The risks identified in the NCC report include making it easier and more efficient to manipulate people through creating personalised and/or conversational advertising. Presently, the NCC report notes that "publicly available generative AI has been largely ad-free, but this is poised to change. In March 2023, Microsoft announced that it would be rolling out paid ads in the Bing chatbot. In May, Google announced that it would integrate advertising in their generative AI products". Reference should be made here to EQ10 concerned with the impact of new and emerging technologies and digitalisation on the EU consumer law framework. Further detail on generative AI and the associated risks from a consumer protection perspective are provided in the June 2023 NCC report.

A further important point raised in the NCC report is that *"there are rising concerns about*

⁴¹¹ <https://www.allenoverly.com/en-gb/global/news-and-insights/publications/generative-ai-and-the-eu-ai-act-a-closer-look>

⁴¹² "Ghost in the machine – Addressing the consumer harms of generative AI" (2023), Norwegian Consumer Council - <https://www.forbrukerradet.no/side/new-report-generative-ai-threatens-consumer-rights/>

generative AI in chatbots and their ability to trick consumers into sharing personal data, which may be repurposed to serve targeted advertising or to manipulate consumers into purchasing products or services. While this challenge echoes a broader debate about the repurposing of personal data for business gains, the manipulative aspects of generative AI models pretending to be humans, as mentioned above, could exacerbate the problems. This is especially relevant in the case of vulnerable groups such as children or lonely people, who may be more likely to share sensitive information about themselves in conversation with the generative AI.”

3.5.5 e-Commerce Directive

EU legislation	Introduction and linkage with EU consumer law
<p>The e-Commerce Directive (Directive 2000/31/EC on Electronic Commerce)</p>	<ul style="list-style-type: none"> • The e-Commerce Directive is a longstanding piece of EU law dating from 2000. The Directive aims to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States. • The Directive is relevant to some areas also regulated through EU consumer law, albeit indirectly, such as influencer marketing. • The DSA builds on some of the core principles in the e-Commerce Directive by regulating digital services and aims to reform the e-commerce legal framework able to respond to new digital challenges. • The DSA does not replace the e-Commerce Directive. However, to achieve greater harmonisation, the DSA incorporates the existing liability exemption rules of the e-Commerce Directive which ensure that intermediary services can continue to thrive in the single market.

The e-Commerce Directive has relevance today to specific topics relevant to digital fairness such as novel forms of marketing.

Art. 6 provides for a basic rule of disclosure and identifiability for commercial communication. Upon adoption, this rule played a role in a variety of marketing strategies in the digital environment where an adequate identification of the commercial communication as such was missing or elusive (spam, advertising in social networks, text messages, etc). Interestingly, this rule still represents today a helpful tool in more recent forms of marketing in the digital economy, such as influencer marketing. As per this Art. 6 ECD, influencers in Europe are required to tag their communications as commercial distinguishing them from the non-commercial ones and mention their commercial partnership, as well as the company for which this communication is made. This is in common with the UCPD and AVMSD.

Coherence with UCPD, not only in terms of policy goals, but in the formal aspects of coordination is ensured. Lack of compliance with the information requirements provided for Union laws on commercial communication, advertising, or marketing is considered an omission of material information that a consumer needs (as per Art. 7 UCPD). Annex II UCPD lists those Union laws relevant to that end, including Art. 6 ECD.

The UCPD’s rules on hidden advertising also cover influencer marketing. There is no legal coherence issue *per se*. It is more a matter of whether it remains coherent to cover hidden ads through the general provisions of the UCPD as opposed to introducing specific rules to strengthen transparency on the rules for influencers and content creators. This issue was considered in the influencer marketing case study and in influencer marketing as a topic within the problematic practices section within effectiveness.

3.5.6 GDPR

The GDPR requires personal data processing to be based on a lawful legal basis, such as consent, necessity for the performance of the contract, or to be of legitimate interest. Some Articles in the GDPR are relevant to the application of EU consumer law:

- Art. 7 outlines the conditions for using consent as a legal basis.⁴¹³
- Art. 9(1) concerns the processing of special categories of personal data. The GDPR applies to the processing of personal data and this article specifically relates to the processing of sensitive personal data.⁴¹⁴ This is relevant to the UCPD's application as personal data-driven commercial practices have become ubiquitous. Issues around the use of personal data for personalised advertising and personalised pricing have become more prominent in policy discourse (two case studies dedicated to this topic have also been prepared – see case study annex). Art. 5(3) UCPD provides protection for vulnerable consumers such as to apply the average consumer test within a particular group in the context of the specific vulnerabilities (e.g. age, credulity, physical or mental infirmity). This is relevant in preventing certain types of behavioural advertising that are exploitative of vulnerable consumers. However, there is no explicit reference to data processing in relation to vulnerable groups despite the relevance of the GDPR's Art. 9(1) in relation to sensitive data.
- Art. 12-14 pertain to transparency requirements. To control the way in which data is processed, the GDPR recognises a number of different rights that data subjects have, including transparency and fairness. These principles are also hallmarks of the UCPD.
- Art. 12 concerns transparent information, communication and modalities for the exercise of the rights of the data subject. Art. 13 outlines the information to be provided where personal data are collected from the data subject. Of relevance is Art. 13(1)(c), the purposes of the processing for which the personal data are intended as well as the legal basis for the processing. Art. 14 outlines the information to be provided where personal data have not been obtained from the data subject. Of particular relevance are points 14(1)(c) through to 14(1)(f):

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; d) the categories of personal data concerned; e) the recipients or categories of recipients of the personal data, if any; and f) where applicable, that the controller intends to transfer personal data to a recipient in a third country [...].
- Art. 17 outlines the specific circumstances under which the right to be forgotten applies. An individual has the right to have their personal data erased if they withdrew consent and there is no other legal ground for the processing, or if the personal data is no longer necessary for the purposes originally collected or processed for. This is important in the context of consumers' control over the future uses of their (personal) data.⁴¹⁵ This Article in the GDPR is relevant to both the CRD and the UCTD. For the CRD, it is relevant to the right to have data erased after a consumer has withdrawn from a contract having exercised their RoW.

⁴¹³ Consent must be unambiguous, which means it requires either a statement or a clear affirmative act. Consent cannot be implied and must always be given through an opt-in, a declaration or an active motion, so that there is no misunderstanding that the data subject has consented to the particular processing. <https://gdpr-info.eu/issues/consent/>

⁴¹⁴ GDPR – Art. 9(1). Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

⁴¹⁵ The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data (2014), Alexander Tsesis Loyola University Chicago, School of Law <https://lawcommons.luc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1502&context=facpubs>

This Article is also relevant to the UCTD. A study for the EP's JURI Committee "*Update the Unfair Contract Terms Directive for Digital Services*" considers the relationship between the UCTD and other EU legislation, including the GDPR.⁴¹⁶ When a consumer decides not to conclude or perform a contract or the DSP terminates a contract, it could be argued that the personal data of the consumer that has already been shared, as part of a payment for the provision of digital services, should be erased pursuant to Article 17(1)(a) GDPR.

- Art. 22 on automated individual decision-making, including profiling, gives the data subject the right not to be subject to a decision based solely on automated processing which produces legal effects concerning him or her or similarly significantly affects him or her. Another interplay between UCTD and GDPR arises from the extent of Art. 22 GDPR.

According to the JURI study report, the EP has argued that consumers should "*not only be informed about how automated decision-making systems work, but also 'about how to reach a human with decision-making powers, and about how the system's decisions can be checked and corrected.'*" They recommend "*recognising the obligation of DSPs to facilitate such human contact points for consumers and human oversight over the automated decision-making. If DSPs terms and conditions envisage only providing consumers with a contact option through the use of virtual assistants and chatbots, this could be considered an unfair term*". The study suggests that this would be contrary to Article 22(1) GDPR.

Furthermore, personalised pricing could trigger the application of the GDPR's Art. 22, given that individuals have the right not to be subjected to automated individual decision-making, including profiling, which produces legal effects or significantly affects them. Under the MD, traders are required to inform consumers clearly when the price they are presented with has been personalised through automated decision-making. According to some observers, there remain some areas of legal uncertainty. "*It is not clear how the requirement of consent for automated decision-making will be implemented in relation to personalised prices or to what extent such practices could be based on the legitimate interests of the business (if and when the effects of automated decision-making could be considered insignificant).*"⁴¹⁷ Also, when a business chooses to implement a pricing model based on prices automatically adapted to the profile of the customer, it should first analyse if they ensure compliance with GDPR's requirements such as: providing consumers with information about the processing, applying the right legal basis and ensuring its implementation, providing an effective execution of the right to access, rectify, or erase personal data and implement appropriate technical and organisational measures.

Reference should also be made to the case study on price personalisation, which considers key issues and reviews the applicable legal framework, and interaction between the GDPR and the UCPD.

The GDPR's role in price personalisation matters has been addressed in some academic research papers, including the issue of the applicability of Art 22. Some research has claimed that the GDPR implicitly grants the right to be offered an impersonal price (not based on personal data processing), which could be made explicit via legislative reform, to increase legal certainty.

Further feedback was received from a legal academic during the interviews that being informed about price automation under the GDPR and personalised prices being used by

⁴¹⁶ Study to Update the Unfair Contract Terms Directive for Digital Services (2021), EP's JURI Committee, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU\(2021\)676006_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf)

⁴¹⁷ <https://www.gnp.ro/ioana-stoica-is-there-any-overlap-between-the-omnibus-directive-and-the-general-data-protection-regulation/>

platforms due to the recent MD changes, there may be greater transparency but it is still unclear for the consumer whether the price impact is negative, neutral, or positive.⁴¹⁸

3.5.7 e-Privacy Directive

EU legislation	Introduction and linkage with EU consumer law
<p>e-Privacy Directive⁴¹⁹ and e- Privacy Regulation⁴²⁰</p>	<ul style="list-style-type: none"> • The e-PD is a longstanding piece of EU law that aims to protect consumers in respect of their electronic communications and helps to protect their privacy. • Whereas the e-PD was adopted in 2002, the e-PR proposal was put forward in 2017. However, the e-PR has not yet been adopted, creating some regulatory uncertainty as it influences what type of data can legitimately be collected by traders via websites, apps, etc. using cookies and user statistics. • The e-PD could be considered outdated to a certain extent since the Directive pre-dates the GDPR. There have been significant technological, market and regulatory developments since 2001.

The e-Privacy Directive complements the GDPR regarding the processing of personal data in the electronic communication sector, as it facilitates the free movement of such data and of electronic communication equipment and services. Article 5(3) of the e-PD requires the user's consent when 'cookies' or other forms of accessing and storing information on an individual's device (e.g. tablet or smartphone) are used, except where such storage or access is necessary for carrying out the transmission of a communication or for the provision of an information society service explicitly requested by a user.

The Proposal for an e-Privacy Regulation would continue to ensure respect for private life and the protection of personal data. The e-PR includes a proposal in relation to the lawful processing of metadata.⁴²¹ Given the volume of data collected about consumers, metadata is also an important consideration for ensuring consumers' privacy because it can reveal information about the content and context of a file, even if a file itself does not contain any identifiable information. The e-PR would, if adopted, regulate certain aspects of cookies and other tracking technologies, including that cookies may only be placed on a user's device with prior consent. Given that data collection is increasingly important in the digital economy, the issue of tracking and whether consumers' privacy should require opting in has been prominent in regulatory debates. As noted earlier under the DMA, gatekeepers must ensure they receive consent from end-users to be able to use tracking technologies (e.g. Art. 5(2) DMA).

While a violation by the trader of the ePrivacy Directive shall not *per se* always amount to be deemed an unfair practice under the UCPD, such privacy and data protection violations should be considered when assessing the overall unfairness of commercial practices under the UCPD. For instance, whether the infringement of the ePrivacy Directive has enabled the trader to use the data for commercial purposes such as direct marketing, profiling, or personalized pricing. From the UCPD perspective, transparency issues will be relevant. Under Articles 6 and 7 of the UCPD, traders should not mislead consumers on aspects likely to impair their decisions such as the commercial intent of certain practices (Article 7(2) and ap. 22 of Annex

⁴¹⁸ The GDPR enshrines the right to the impersonal price (2022), Fabrizio Esposito,

Computer Law & Security Review, Volume 45, (<https://www.sciencedirect.com/science/article/pii/S0267364922000085>)

⁴¹⁹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

⁴²⁰ Proposal for an ePrivacy Regulation - <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation>

⁴²¹ Metadata is data that describes other data, such as the author, date created and location. It has a high privacy component and should be anonymised or deleted if users did not give their consent, unless the data is needed for billing.

l). Moreover, the information requirements laid down by e-Privacy Directive may be considered as material information under the UCPD Article 7(5). Consequently, pursuant to Article 7(2) and as per point 22 of Annex I UCPD, not informing a consumer that the data provided or collected by cookies are to be used for commercial purposes or certainly not obtaining consent to do so could be considered a misleading omission of material information.

Some feedback on the coherence of the e-PD with EU consumer law was received. In the ongoing discussions on the proposed ePrivacy Regulation, an EU business association mentioned in their targeted response that *“companies should be able to rely on legal bases other than consent for ad performance measurement as part of their legitimate business interest to measure the effectiveness and competitiveness of their campaigns.”* However, consent is not always required if it is necessary if the cookies are necessary for audience measurement (analytics) if the measurement is done by the provider of the service requested by the end user or by third-party cookies on behalf of the service provider or jointly.

3.5.8 Data Act

EU legislation	Introduction and linkage with EU consumer law
<p>Data Act (Regulation (EU) 2023/2854)⁴²²</p>	<ul style="list-style-type: none"> • The Data Act entered into force on 11th January 2024. • The Regulation established a harmonised framework for data sharing in the EU. The purpose was to harmonise rules on fair access to, and the use of such data and thereby to create a fair and competitive data market by facilitating data sharing and use. • The Regulation covers both B2B and B2C. Whilst its scope covers both personal and non-personal data, there is a strong focus on the latter. The Data Act must be applied in conjunction with the GDPR, which governs personal data access and use rights for data subjects. EU consumer law (indirectly) addresses personal data but not non- personal data. • The Regulation also protects European businesses from unfair contractual terms in data sharing contracts that one contracting party unilaterally imposes on the other.

The Data Act puts obligations on manufacturers and service providers to let their users, either companies or individuals, to access and use the data generated using their products or services. It establishes a framework regarding the conditions and extent to which access to and use of data generated by connected products or related services should be allowed for subjects other than the manufacturer or holder of the information.

It allows users of connected devices, ranging from smart household appliances to connected and autonomous vehicles (CAVs) to gain access to data generated by their use. As such, the Data Act gives consumers and companies more control over what can be done with non-personal data, clarifying who can access the data and on what terms. The portability of data is also addressed.

Prior to the Data Act, data generated from products was often exclusively collected and harvested by manufacturers and service providers. Regarding Internet of Things (IoT) data, the new law focuses on the functionalities of data collected by connected products instead of the products themselves. It introduces the distinction between ‘product data’ and ‘related service data,’ from which available data can be shared. The emphasis in the Data Act is on

⁴²² 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).

addressing fairness in the allocation of the value from data, which has analogous relevance for EU consumer law.

- Art. 2(1) defines 'data' as any digital representation of acts, facts or information and any compilation of such acts, facts, or information, including in the form of sound, visual or audio-visual recording.
- Art. 3 outlines the obligation to make product data and related service data accessible to the user, including by designing connected products and related services in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user.

Various relevant elements for consumer protection are contained in this provision. Beyond the strong framework for personal data, the Data Act expands the protection to non-personal data in relation with smart products (product data, related service data). Interestingly, the provision refers, as in the DSA, to machine-readable format.

There are also pre-contractual information requirements for instance in relation to Art. 3(2) 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). This 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.

This type of information could also be of use to consumers in relation to their personal data which would align consumers' interest as protected by personal data law with the Data Act. However, if such pre-contractual information were to be added to contractual T&Cs, it could risk information overload, given that consideration is also being given to simplifying T&Cs to improve digital fairness by improving the clarity and ease of comprehension of key T&Cs by consumers.

- Art. 4 outlines the rights and obligations of users and data holders with regard to access, use and making available product data and related service data. Users should either be able to access their data directly via a connected device or upon request.
- Art. 7 clarifies the scope of business-to-consumer and business-to-business data sharing obligations, exempting data generated through connected products manufactured or designed or related services provided by a microenterprise or a small enterprise.

As the Regulation mainly deals with non-personal data generated through the use of products, there do not appear to be any major incoherence issues, as the UCPD's main sphere of interest is to prevent unfair, misleading and deceptive practices, including in respect of personal data. The Data Act is without prejudice to the applicability of other EU legislation, such as the GDPR and consumer law, which must be applied in parallel.

The Data Act's focus is on a series of issues that are important from a consumer data protection perspective, such as non-personal data holders' rights in terms of data access and portability, giving users more rights to have more control over their data, such as being able to access their own data upon request, coverage of meta data and issues around data use. The focus on data fairness, non-discriminatory T&Cs and on transparency is of general relevance when considering how best might EU consumer law deal with data access and use.

Presently, however, it can be noted that there is a lack of explicit provisions in consumer law relating to personal data protection, data sharing, portability etc.

BEUC developed a position paper in October 2022 on the EU Data Act⁴²³, in which they advocated that consumers must be protected by design and by default. *“Certain contractual clauses should be prohibited for B2C contracts, such as bundling necessary and unnecessary purposes of processing. The Data Act should not only prohibit the use of dark patterns by third parties, but also by data holders.”* The paper also suggested that *“Consumers must be in control of data generated through the use of products and related services. This for instance requires meaningful consumer choices according to their preferences and an enhanced data portability right with clear format and interoperability conditions.”* Among the implications for EU consumer law, according to BEUC, were that the issue of data access and portability could be addressed as part of a comprehensive consumer law package in future that could address inter-related issues relating to the use of personal data.

Lastly, whilst the Data Act prohibits unfair contractual terms unilaterally imposed that deviate from good commercial practice, this relates to B2B data sharing and transactions.

3.5.9 Audiovisual Media Services Directive

EU legislation	Introduction and linkage with EU consumer law
<p>Audiovisual Media Services Directive (AVMSD)⁴²⁴</p>	<ul style="list-style-type: none"> • The AVMSD ensures the proper functioning of the single market for audiovisual media services, while contributing to the promotion of cultural diversity and providing an adequate level of consumer and protection of minors. • Directive 2010/13/EU was updated in 2018. The new rules in the revised AVMSD aim to create a regulatory framework fit for the digital age, leading to a safer, fairer, and more diverse audiovisual landscape. The Directive was adapted to reflect the advanced convergence of audiovisual media services and current technological developments. • The Directive’s scope was also extended to the digital age in terms of the types of traders to whom the rules are applicable. The revised Directive extended the scope to include video-sharing platform services (“VSPS”) (for example, YouTube and Vimeo). • Product placement, sponsorship and surreptitious advertising are subject to both specific audiovisual media related legislation, but also to consumer law.

Under Articles 9-10, the AVMSD bans deceptive audiovisual design, such as surreptitious advertising, subliminal techniques, and regulates the identification of sponsored programmes and product placement. The aim is to make viewers aware of being targeted with commercial ads such that they can make informed decisions. This addresses the problem of covert targeted ads by certain influencers that mix commercial and non-commercial content.

The AVMSD’s scope is narrower than EU digital laws in that it prohibits the intentional display of surreptitious ads and/ or subliminal techniques. These information and transparency requirements share some similarities with the UCPD’s rules on hidden ads, but in the AVMSD, the rules are specific to audiovisual content and certain types of traders. Surreptitious ads

⁴²³ [Giving consumers control of their data: BEUC position paper on the Data Act proposal](https://www.beuc.eu/general/privacy-and-personal-data-protection) BEUC, October 2022, <https://www.beuc.eu/general/privacy-and-personal-data-protection>

⁴²⁴ Codified version of the revised AVMSD from 2018 - <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32010L0013>

and/ or subliminal techniques are not expressly prohibited in EU consumer law, but rather covered through the UCPD's general provisions.

The AVMSD includes specific disclosure requirements which require that commercial partnerships are mentioned in all communications and commercial communications are identified as such, including in audiovisual media service or programmes and on video-sharing platforms (Article 28b).

The AVMSD also covers influencer marketing as influencers are among the traders targeted that are creators of audiovisual content. The information requirements are not duplicative *per se*, but rather complementary to and reinforcing of those in the UCPD.

Regarding the degree of regulatory certainty between how the rules on influencer marketing should be applied in different pieces of EU law, concerns were expressed among some stakeholders about diverging interpretations of influencers under the UCPD and AVMSD by the relevant respective authorities. For instance, the Dutch Media Authority is only enforcing rules against influencers with more than 500k followers, using the AVMSD as a legal basis, whereas the Dutch Consumer and Market authority does not limit itself to follower counts and applies the UCPD to everyone. Similar debates regarding the number of followers that should denote a professional social media influencer have taken place in Scandinavian countries. As expounded above, the DSA also addresses influencer-related issues as it provides for the obligation of online platforms to provide a functionality for any recipient of the service to declare that the content they post or provide is or contain commercial communication.

Under Article 6(1)(a) and Article 28b(1)(a), the AVMSD obliges Member States to take appropriate measures to protect minors from audiovisual content which may impair their physical, mental, or moral development. Such measures may include selecting the time of the broadcast, age verification tools or other technical measures. Under Article 9, minors should not be the target of commercial communications about alcoholic beverages, direct exhortations to buy products, unreasonably show minors in dangerous situations etc. The AVMSD also encourages co-regulation and self-regulation regarding inappropriate audiovisual commercial communications for unhealthy foods and beverages (Article 9(4)).

The AVMSD governs EU-wide coordination of national legislation on all audiovisual media. A challenge in terms of effective coordination with consumer law is that the Directive is implemented using minimum harmonisation whereas the UCPD follows maximum harmonisation, as noted by some stakeholders in their targeted consultation responses.

In the targeted consultation, there was some feedback that some stakeholders in the audiovisual sector were concerned that the AVMSD is a minimum harmonisation Directive allowing a lot of flexibility for MS to legislate through additional rules, in contrast with the UCPD, a maximum harmonisation Directive. However, the minimum harmonisation character of the AVMSD was not found to have weakened consumer protection, given that the UCPD provides a backstop to legislate unfair practices and already provides protection relating to ensuring transparency in social media marketing practices, including by influencers.

Overall, there do not appear to be coherence problems between the AMVSD and EU consumer law. However, there is a risk of diverging interpretations when courts, media authorities and CPAs interpret the same obligations concerning the transparency of commercial communications in a different manner, for example as regards influencers.

3.5.10 Fundamental rights and equalities legislation

The Charter of Fundamental Rights of the European Union (the 'Charter') sets out fundamental rights which are relevant to the application of EU consumer law, such as the respect for privacy (Article 7), rights of the child (Article 24) and a high level of consumer protection (Article 38).

The attention given in the Charter to protecting the rights of children raises issues as to whether children (or the broader concept of minors) should be more explicitly protected in EU consumer law in future than they are presently. Related issues are examined in the thematic review of the treatment of the protection of children's rights in EU legislation and consumer law.

Turning to equalities legislation, the EU equality directives do not cover all grounds and fields of discrimination. Discrimination in access to, and the supply of goods and services based on age, sexual orientation, religion, or beliefs is not covered. The 2008 proposed Equal Treatment Directive (also known as the Horizontal Directive as it covered all equality grounds) has not been adopted yet, which would have expanded protection against discrimination on the grounds of age, disability, religion or belief and sexual orientation to the areas of social protection, healthcare, education, housing and access to goods and services. These four grounds are currently only covered regarding employment and vocational training.

An interplay with consumer law emerges to the extent that discrimination on the mentioned grounds in access to, and the supply of goods and services, entails a discriminatory situation of a person as a consumer, that is, in their position vis-à-vis a trader and in relation to the access to services or goods. In that regard, EU equality directives do contribute to the protection of consumers by avoiding and mitigating discriminatory risks. Coherence in the extent and the scope is desirable.

Secondly, the Directive on gender equality (Directive 2004/113) in access to and supply of goods and services excludes 'advertising' from its scope meaning that there are no protection rules specifically regarding gender-related ads.

Thirdly, stereotypical content in advertisements (without this leading to discrimination in a particular area per se) is not covered by EU equality legislation. This raises questions as to whether EU equality legislation should be updated to reflect these perceived legal gaps, or whether EU consumer legislation could instead address some of these issues. Interestingly, it may be discussed whether EU equality legislation is also aimed at countering vulnerabilities and in that regard equality rules are contributing to the protection of vulnerable consumers. Nonetheless, as explained in the case study on consumer vulnerability, however, a challenge is that consumer law is applicable to all consumers, and people may have multiple vulnerabilities and/ or multiple personal characteristics (e.g. a person with disabilities who is also from an ethnic minority background). The UCPD's Art. 5(3) is presently confined to covering various aspects of vulnerability, such as age, credulity, mental or physical infirmity, etc.

3.5.11 Accessibility Act

EU legislation	Introduction and linkage with EU consumer law
<p>The European Accessibility Act (EAA)⁴²⁵</p>	<ul style="list-style-type: none"> • The EAA has been developed off the back of the UN Convention on the Rights of Persons with Disabilities (UNCRPD). Specifically, the EAA aims to improve the functioning of the internal market for accessible products and services, by removing barriers created by divergent rules in Member States.⁴²⁶ Moreover, specific consideration has been made within the EAA in relation to the digital environment. • Within the development of this legislation, a focused selection of products and services that are most important for persons living with disabilities, related to – and/or facilitating – their engagement with the digital

⁴²⁵ [Directive - 2019/882 - EN - EUR-Lex \(europa.eu\)](#)

⁴²⁶ [European accessibility act - Employment, Social Affairs & Inclusion - European Commission \(europa.eu\)](#)

EU legislation	Introduction and linkage with EU consumer law
	<p>environment, these include:</p> <ul style="list-style-type: none"> • Computers and operating systems • ATMs, ticketing, and check-in machines • Smartphones • TV equipment related to digital television services • Telephony services and related equipment • Access to audio-visual media services such as television broadcast and related consumer equipment • Services related to air, bus, rail, and waterborne passenger transport • Banking services • e-books • e-commerce

Under the EAA, service providers have to ensure that they design and provide services in accordance with the accessibility requirements of this Directive. Article 2 clarifies the application of the EAA across services providing audiovisual media services, and for e-books and their related software. The inclusion of e-books and audio-visual media services has a clear implication for B2C contracts and subscriptions within the digital environment - it reaffirms here and through *Annex I Accessibility Requirements for Products and Services* the need for transparency and clear presentation of terms for consumers.

The four principles of perceivability, operability, understandability and robustness underlying the EAA in relation to website accessibility, stem from the Web Accessibility Directive⁴²⁷ and directly guide developers and platforms in relation to the principles of fairness by design and by default. EAA Articles 7, 8 and 9 duly place the burden of compliance and proof of product conformity upon supply-side actors in the production chain as is considered appropriate in each case (the manufacturer or recognised representative, the importer, the distributor).

During interviews, major platforms and technology developers pointed to the five-year implementation period of the Accessibility Act (concluding in 2025) as a further contributor towards the ongoing legal uncertainty with regards to the anticipating and mitigating issues in compliance with the EU consumer law acquis.

In relation to vulnerable consumers and the potential for further obligations upon traders in EU consumer law, one major platform and technology trader questioned the ability and feasibility of traders to provide tools for these consumers given the difficulty in identifying “mental infirmity and credulity.” However, the EAA’s universal application will seemingly help to resolve this as it reinforces the principles of fairness and transparency by design and default. It is interesting to note how the UCPD and the EAA approach the problem of accessibility from opposing angles. While the EAA follows a promoting and enabling approach, the UCPD takes a limiting approach by determining unfairness in cases of vulnerability.

3.5.12 Distance Marketing of Financial Services (DMFSD)

EU legislation	Introduction and linkage with EU consumer law
<p>Distance Marketing of Financial</p>	<ul style="list-style-type: none"> • Directive (EU) 2023/2673 amending Directive 2011/83/EU was adopted on

⁴²⁷ Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies

EU legislation	Introduction and linkage with EU consumer law
<p>Services (DMFSD)⁴²⁸</p>	<p>22nd November, 2023.⁴²⁹</p> <ul style="list-style-type: none"> • Member States have two years to implement the rules into national law and a further six months to apply them (i.e. as from 19 June 2026). • Directive (EU) 2023/2673 has extended the CRD's scope to cover financial services contracts concluded at a distance. This should ensure the necessary complementarity between specific rules on financial services concluded at a distance and the more general requirements in the CRD. • The new Directive modernises the CRD by incorporating relevant articles from Directive 2002/65/EC, which has been repealed. It extends certain rules of the CRD to consumer financial services concluded at a distance and introduces new provisions to ensure online fairness when consumers conclude financial services online. • A withdrawal function/button for all distance contracts to exercise the RoW was introduced due to these regulatory amendments, and this is applicable to all sectors, not only financial services to make it easier for consumers to exercise their RoW.

The DMFSD introduces a right of withdrawal button for all distance contracts in Article 11a CRD. The withdrawal function shall be labelled with the words “withdraw from contract here” or an unambiguous corresponding formulation in an easily legible way. The withdrawal function shall be continuously available throughout the withdrawal period. It shall be prominently displayed on the online interface and easily accessible to the consumer. Traders must also send consumers a confirmation of their withdrawal.

The DMFSD also introduces the right of access to a human interlocutor in Art. 16d(3) CRD. Where a professional uses online tools in the context of concluding distance financial services contracts (e.g. robo-advisors or chatbots), Member States shall ensure that the consumer shall have 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**, in the same language as that used for the pre-contractual information provided in accordance with Article 16a(1).

The DMFSD also introduced a **dark patterns prohibition provision in Article 16e CRD in the context of concluding financial services contracts at a distance.** The recitals provide additional detail regarding how dark patterns in interface design limit consumers' choices. Recital 41 notes that *“Dark patterns on traders’ online interfaces are practices that materially distort or impair, either on purpose or in effect, the ability of consumers who are recipients of the financial service to make autonomous and informed choices or decisions [.....]”*. It then explains that *“Traders should therefore be prohibited from deceiving or ‘nudging’ consumers who are recipients of their service and from distorting or impairing their autonomy, decision-making, or choice via the structure, design or functionalities of an online interface or a part thereof”*.

The Article specifies that Member States shall adopt measures that address at least one of the following practices by traders: (a) giving more prominence to certain choices when asking the consumers who are recipients of their service for a decision; (b) repeatedly requesting that consumers who are recipients of the service make a choice where that choice has already

⁴²⁸ https://finance.ec.europa.eu/consumer-finance-and-payments/retail-financial-services/distance-marketing-financial-services_en

⁴²⁹ Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023L2673>

been made, especially by presenting pop-ups that interfere with the user experience; or (c) making the procedure for terminating a service more difficult than subscribing to it.

These changes have helped to modernise and update the CRD for the digital age in respect of financial services concluded at a distance. However, there could be benefits in extending these provisions to cover all contracts concluded at a distance given that dark patterns are prevalent in many sectors outside of financial services.

From a coherence perspective, if the basic legal principle is that it should be as easy to enter a contract as it is to withdraw from it, as per the new withdrawal function/button for all distance contracts, this raises a broader coherence issue as to whether a cancellation button should also be introduced in respect of the cancellation of contracts beyond 14 days and when these are up for renewal. This issue is explored in the problematic practices section under effectiveness and in the subscriptions case study.

As regards the dark patterns prohibition, there are concerns about the interplay between the CRD provision and the UCPD, which can capture all dark patterns, including the three choices of practices that were presented to the Member States.

As the Directive was adopted in November 2023, there was limited feedback on coherence issues in the DFMSD. There was feedback on the merits and drawbacks of a withdrawal button and a possible cancellation button (the latter as per national legislation in DE), but this relates to effectiveness rather than coherence.

3.5.13 General Product Safety Regulation (GPSR)

EU legislation	Introduction and linkage with EU consumer law
<p>General Product Safety Regulation (GPSR)</p>	<ul style="list-style-type: none"> On 23 May 2023, Regulation (EU) 2023/988 on general product safety was published. This replaced the longstanding GPSD. The purpose of the GPSR is to ensure product safety to provide high levels of consumer protection whenever specific sectoral legislation applicable to products is absent. The GPSR modernised the GPSD, including updating it for the digital age, given that it now covers software updates, cybersecurity, product safety when shopping via online marketplaces. The GPSR builds on the recently adopted DSA, horizontal rules that regulate online content and products.

The GPSR provides that *“when assessing the safety of digitally connected products likely to have an impact on children, manufacturers should ensure that the products they make available on the market meet the highest safety standards of safety, security and privacy by design, in the best interests of children.”* Recital 5 notes that: *“Dangerous products can have very negative consequences for consumers and citizens. All consumers, including the most vulnerable, such as children, older persons or persons with disabilities, have the right to safe products.”*

Manufacturers will have to perform a risk assessment which should take into consideration products used by vulnerable groups of consumers, such as children, old people, and those with disabilities. The Regulation considers the ‘reasonably foreseeable use’ of products but which should consider that children may use products in unforeseeable ways posing additional risks.

The GPSR also stresses the relevance of mental health risks and the need for ensuring safety by design: *“The assessment should take into account the health risk posed by digitally connected products, including the risk to mental health, especially of vulnerable consumers,*

in particular children. Therefore, when assessing the safety of digitally connected products likely to have an impact on children, manufacturers should ensure that the products they make available on the market meet the highest standards of safety, security and privacy by design, in the best interests of children.”

BEUC suggested in a position paper at the need for closing regulatory loopholes related to a lack of sufficient information on the identify of third-party vendors purchased via online marketplaces.⁴³⁰ It can be noted that the DSA has already partially addressed this issue by requiring providers of online platforms allowing consumers to conclude distance contracts with traders to obtain certain information of traders (Art. 30 DSA, traceability) in third countries who promote or offer products or services to consumers located in the Union. Article 31 also obligates B2C platforms to randomly check if the products or services offered by their online retailers are listed as illegal. The DSA also introduced the right to information related to illegal products (Art. 32 DSA). Moreover, through the MD, there were additional information requirements relating to disclosure requirements relating to the identify of traders on online marketplaces. This has helped to improve information available to consumers about the identify of traders.

The additional protections provided to consumers in the GPSR are coherent with EU consumer protection law. However, the GPSR is safety-focused and therefore includes more detailed provisions specifically relating to digitally-connected products and the associated risks for vulnerable consumers. Such risks for consumers specific to the digital environment are not presently mentioned in EU consumer law.

The GPSR in contrast with the GPSD now provides redress rights to consumers through representative actions (Art. 39), similarly to the UCPD (the MD added a new Article 11a to the UCPD on redress rights for consumers harmed by unfair commercial practices).

The importance of protecting children (or minors depending which terminology may be considered more appropriate as this varies between different pieces of EU law) within the GPSR is of interest from a consumer law perspective. The Regulation explicitly stresses the importance of protecting children as a category of vulnerable consumer in respect of their usage of products, including digitally-connected products in terms of safety, cybersecurity, and privacy. The latter two areas are also important in the application of EU consumer law in the digital environment. Without adequate cybersecurity and privacy, children are at greater risk of exploitation, from manipulative and deceptive practices.

The age suitability for children of products (including digitally connected products) is addressed in the GPSR. By extension, the age suitability for children of digital services could be considered in the UCPD as an additional protection measure to strengthen coherence of the EU legal framework overall. It can be noted that some MS have recently tried to introduce age rules in respect of the use of certain digital services, such as young children and teenagers using social media without parental permission, although such legislation is controversial by some stakeholders with concerns over its potential efficacy. Nonetheless, it is worth noting that any reference to age-appropriate design of products and services in the digital environment is presently missing in EU consumer law.

3.5.14 Thematic issues

Whilst the interaction between EU consumer law and other relevant pieces of law was considered in the previous section, it is important to consider certain **horizontal thematic topics** as a combination of different pieces of EU consumer law and other pieces of EU law

⁴³⁰ A New General Product Safety Regulation, BEUC/ ANEC, Sylvia Maurer and Florence Punzano
https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-092_A_New_General_Product_Safety_Regulation.pdf

are applicable, notably the regulation of consumer data, protection of minors and dark patterns.

3.5.14.1 Consumer data

The specific regulatory challenges of protecting consumer's data in the digital world should be recognised, which stem from the different regulatory approaches taken in different areas of law, and the challenges in combining these in an effective way that ensures high levels of consumer protection in the digital environment. *"The protection of consumer data is an issue that cuts across many areas of the law that used to be very distinct and often in regulatory competition. The legislations in place do not, by and large, acknowledge each other's existence or, if they do, they do not always articulate in a detailed manner how the competing regimes may apply in tandem".*⁴³¹

There are differences and similarities between EU consumer protection and data protection laws. *"While consumer protection law can be seen to merely set a floor in its pursuit of a sufficiently high level of consumer protection, data protection law – due to its clearly articulated dual purposes of (a) protecting individuals with regard to the processing of personal data and (b) providing for the free movement of such data – sets both a floor and a ceiling".*

There is a lack of clear connection between the rules on data protection, in particular GDPR, and EU consumer law. This is the case for some substantive rules, such as those on dark patterns. Moreover, the **inter-relationship between the UCPD and GDPR** is not presently mentioned in the UCPD's legal text, either in the recitals or the provisions. Rather, issues around applying the GDPR in conjunction with data legislation are explained in the updated UCPD Guidance (Dec 2021) where there is a section on the interplay between the UCPD and the GDPR and e-Privacy Directive. This makes clear that the GDPR must be applied by traders in parallel with the UCPD in relation to the processing of personal data from data subjects. In some academic literature, there are questions as to whether the UCPD is fully effective regarding personal data processing due to the lack of sufficient regulatory clarity as the issues are regulated implicitly rather than in detail. However, this does not mean there are fully-fledged legal gaps, it is more a question of whether the current regulatory framework can continue to be coherent given some legal uncertainties regarding which personal data practices are acceptable, and which are not, and given that other laws such as the DSA codify what is prohibited and what is not. Furthermore, the GDPR and DSA both address the use of sensitive personal data, but the UCPD does not regulate which specific data can be used in personalisation practices, despite their growing ubiquity.

An EU business association responding to the targeted survey pointed out that existing data laws already provide protection in the application of the UCPD. *"Using data subjects' rights under the GDPR, consumers can address any commercial practice involving the processing of consumers' personal data, ranging from personalized marketing communications or the growing use of "free" digital services involving commercial processing of users' personal data".*

Under Art. 26(3), the DSA prohibits targeted advertising using sensitive data (e.g. sexual orientation, religious belief, ethnicity, or racial background) within the meaning of Article 9(1), GDPR. It is therefore prohibited to present profiling-based targeted advertising on online platforms using special categories of personal data. This prohibition based on sensitive personal data only applies to online platforms that present ads on their online interfaces. However, it can be noted that the term "online platform" is widely defined in the context of the DSA as including any intermediaries hosting content, and thus the prohibition already applies broadly across many different types of online services and applications that present ads. However, it remains the case that the DSA is not applicable to all traders, unlike the UCPD,

⁴³¹ Riefa, Christine. Protecting consumer's data in the digital world: Advocating Fairness by Design, University of Reading, School of Law https://unctad.org/system/files/non-official-document/ccpb_Speaking_Notes_Riefa_digital_data_protection_en.pdf

therefore, the **inclusion of similar provisions in the UCPD could help to strengthen coherence and the uniformity of application.**

Some stakeholders, such as consumer associations and Ministries, have argued that as per the DSA's Art. 26(3) on the use of sensitive data and Art. 28(2) on the prohibition of personal data for profiling minors, similar provisions should also be included in the UCPD to strengthen coherence and provide regulatory certainty. Without this extension, there may be regulatory uncertainty and uneven levels of protection for minors as they would be protected when using online platforms but not explicitly when using other websites and apps (such as video games) in the digital environment.

A legal academic commented in the targeted consultation in respect of the GDPR that data as remuneration remains a bit puzzle especially in terms of how to assess the substantive fairness of the transaction even more when consumers both pay for transactions or give their data.

The UCPD already implicitly deals with personal data processing by online platforms and by third parties that engage in data-driven business practices. *“Considering that personal data is often sold to third parties and de facto has economic value, it is reasonable to assume that data-driven businesses engaging in B2C transactions should always fall under the scope of the UCPD. Besides, whenever an online platform can be considered a trader as regards the UCPD, it is required to act with a degree of professional diligence and not mislead consumers through action or omission. Further, looking at the online platform’s data processing, the protection offered against the unauthorized use of consumer’s data is provided by the transparency requirements set out in the UCPD. An example might be a trader who fails to disclose in a clear, intelligible, and timely manner that personal data provided by the consumer are processed and used for commercial activities of the trader; this would be an unfair omission, defined in the UCPD.”*

There may also be a need for greater clarity across EU laws regarding the purpose for which personalised data is being used for, and therefore what types of data users are consenting to opt in to. For instance, data may be used for personalised ads, but also other forms of data collection and tracking may be used for commercial purposes, and whether gathering data for behavioural analytics is permitted, or if there are specific types of data prohibited.

In recent years, the **degree of coherence between EU consumer law and data laws** has come into sharper focus both in relation to coherence but also through enforcement activities and legal cases as there have been a number of cases that relate to whether digital service providers, platforms and OTT service providers’ business practices in relation to data processing and exploitation for commercial purposes are sufficiently transparent to avoid such practices being unfair or misleading under the UCPD. *“There has been an interest from various national enforcement bodies in remedying commercial behaviour exploiting the increasing information and power between consumers and analytics companies.”*⁴³²

There have been legal cases relating to the inter-relationship between the UCPD and the GDPR in relation to data processing as a pre-condition for being able to use a service.⁴³³ There have also been cases relating to what constitutes a legitimate reason for the processing of personal data if consumers do not agree to the terms and conditions of a service which include the collection and processing of personal data.⁴³⁴ This demonstrates that there are complexities relating to the coherence of the interaction between EU consumer and data laws that still need to be tested through case law, EDPB judgements and CJEU rulings.

⁴³² Nišević, M. (2021). A study on the personal data processing and the UCPD focused on Italy, Germany and the UK. Maastricht Journal of European and Comparative Law, 28(1), 7-29. <https://doi.org/10.1177/1023263X20961493>

⁴³³ Kammergericht Berlin, Judgment of 24 Jan. 2014, 5 U 42/12; available at :

www.vzbv.de/sites/default/files/downloads/Facebook_II_Instanz_AU14227-2.pdf

⁴³⁴ <https://www.dataquidance.com/news/eu-beuc-files-complaint-against-meta-regarding-pay-or>

Regarding the application of the legal framework, coherence-related issues not only relate to the legal provisions but also to enforcement, given that enforcement of data protection legislation under the GDPR falls within the remit of DPAs whereas enforcement of consumer protection rules falls under CPCs, but there is a lack of clarity as to how to effectively enforce cases relating to unfair personal data collection and processing in the digital age. Coordination in enforcement is relevant for improving coherence, insofar as disparities in enforcement of data protection and consumer protection laws may lead to inharmonious interpretation or incoherences de facto.

A stakeholder (an EU business association in video games) stated that:

“As legal frameworks become increasingly interlinked, collaboration and coordination between enforcement authorities must become standard practice. It will ensure a uniform application of the legal framework based on a coherent interpretation of the rules. The Commission should therefore secure that consumer and data protection authorities, for example, provide joint guidance on the interplay and overlapping requirements of these two regulatory frameworks. To ensure legal certainty, they must provide unambiguous definitions for key concepts used across different legislative environments and consistent interpretation of the rules. It is essential to secure that cooperation of this kind includes continued and regular consultation with the industry on how the legal frameworks have been implemented.”

Some stakeholders during the interviews and survey consultations have argued that more should be done to explicitly prohibit the use of personal data about consumer vulnerabilities, such as their psychological traits, that go beyond the concept of sensitive data in the GDPR.

There are concerns among stakeholders regarding the need to safeguard autonomous decision-making of individuals when they are confronted with new technologies and new forms of data gathering that could lead to manipulative advertising, even if subtle. There was broad **stakeholder consensus that behavioural advertising based on psychological and/ or emotional profiling should be explicitly prohibited in EU consumer law**. Currently, neither the GDPR nor the UCPD address the issue of psychotropic profiling explicitly, although the UCPD provides additional protection for vulnerable consumers under Art. 5(3).

Given the crucial importance of both personal and non-personal data (and big data analytics) to many business practices in the digital economy, the regulatory framework should be updated. Effective consumer data protection will require new regulatory approaches that bring together different areas of law e.g. consumer protection, data protection and competition law (Riefa).⁴³⁵ In the view of some legal academics and consumer associations, the legal framework could better tackle the need for data protection and privacy for consumers by placing a positive duty on traders “to behave fairly by design and to make invasive treatment of our data an opt-in rather than an opt-out activity” and by encouraging or requiring traders to deliver “data privacy-friendly solutions.” This centres on the concept of integrating privacy by design into online interfaces, which has been discussed in position papers in response to this study and in some academic research papers.

It should be made clearer in the UCPD how the Directive needs to be applied in conjunction with EU data law through the GDPR and the e-PD/e-PR. As a minimum, it should be mentioned in the recitals of the UCPD the need for traders to apply the Directive in conjunction with relevant EU data laws, and a definition of personal data should be provided in the Directive. Definitions should be for the sake of coherence totally aligned.

It would improve the UCPD’s coherence in the digital age if personal data-driven practices were more clearly regulated in consumer law directly. For example, the DSA’s prohibition of

⁴³⁵ Riefa, Christine. Protecting consumer’s data in the digital world: Advocating Fairness by Design, University of Reading, School of Law https://unctad.org/system/files/non-official-document/ccpb_Speaking_Notes_Riefa_digital_data_protection_en.pdf

sensitive personal data for personalised targeted advertising purposes and of using personal data to create profiles for minors used for ads could be replicated in the UCPD, to extend protection beyond users of platforms to any consumer vis-à-vis all traders and online interfaces.

Some specific provisions should be introduced providing clear rules concerning the interaction between EU consumer and EU data laws. This would provide an opportunity to tailor the more general rules in the GDPR to the specific needs of EU consumer law and achieving high levels of consumer protection, for instance, reflecting the big picture trend of a data-driven European digital economy, and business practices that reflect a strong dependency on personal data. This would strengthen coherence, facilitate enforcement, and reduce legal ambiguity.

Specific suggestions are that the UCPD should cover more clearly the misuse of data such as when data is collected for one purpose under the GDPR but then used for other purposes and that behavioural advertising using psychotropic profiling should be prohibited in the UCPD, and that the collection and processing of sensitive data for profiling purposes should be prohibited to ensure coherence with Art. 9(1) GDPR. The prohibition of the manipulation of sensitive personal data could be mentioned either in the specific legal text or identified as a prohibited practice in the Annex 1 UCPD blacklist.

3.5.14.2 Protection of minors

The European Union has a long tradition of providing special protection to children as consumers. Thirty-five years ago, certain categories of consumers were granted additional levels of protection from advertising through the provisions of the Directive 89/552/EEC on television without frontiers. This Directive was eventually replaced by the AVMSD. Moreover, the CJEU has confirmed the vulnerability of children towards advertising in its decision in *De Agostini*.⁴³⁶ EU consumer law addresses the protection of children and minors to some extent. However, the regulatory approach is centred on defining vulnerable consumers in the UCPD on the grounds of age. In contrast, other recent EU legislation has been more explicit and detailed in providing regulatory protection. Key legal provisions in other EU laws relevant to minors (with potential utility for EU consumer law) are now summarised:

The DSA's Art. 14(3), Art. 28(1), (2) and (3), and Art. 34(1)(d) relate to the protection of minors. Article 14(3) provides that where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand. Article 28 requires providers of online platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service. Under Art. 28(2) providers of online platform are not allowed to present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. Furthermore, under Article 34(d), the risk assessments from VLOPs and VLOSEs cover (d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

The GDPR's Art. 8 provides the conditions applicable to a child's consent in relation to information society services. This is a prerequisite for any data processors wishing to process data for the under-16s, otherwise it is illegal. Furthermore, under Art. 25, the requirement for data protection by design and default indirectly covers children. For instance, in relation to connected toys, it would avoid a situation in which toys gather personal data which could be

⁴³⁶ Prohibition of misleading advertising and the prohibition of advertising directed at children - Judgement of the Court of 9 July 1997. *Konsumentombudsmannen (KO) v De Agostini (Svenska) Förlag AB (C-34/95)* and *TV-Shop i Sverige AB (C-35/95 and C-36/95)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61995CJ0034>

used to exploit children or put them in danger. This Article also has relevance to the debate within EU consumer law about whether there should be analogous provisions developed concerned with the concept of achieving digital fairness through compliance by design principles in online interface development, which could also prevent dark patterns.

The e-Privacy Directive protects the confidentiality of communications and terminal equipment of users, including children as part of the fundamental right to respect for private life regarding communications. However, this is not a minor or children-specific rule.

The GPSR addresses minors in relation to the age suitability for children of products and the requirement to carry out a risk assessment of the risks for vulnerable consumers such as children, older people and persons with disabilities. As this covers mental health not only physical safety risks, it arguably covers aspects of digital addiction, even if this is not explicitly referenced in the provisions.

When considering the legal framework to protect children's rights, it can be noted that there are currently no EU laws specifically to tackle digital addiction, although during 2023, the EP's IMCO Committee has been doing work in this area, which has touched upon the addictive design of online services. Arguably, this could also be considered when reviewing EU consumer law provisions in respect of dark patterns. Challenges around digital addiction as a problematic practice are addressed in the effectiveness section and in the case study on digital addiction.

The UCPD's Art. 5(3) refers to the need to assess the fairness of commercial practices from the perspective of average members of vulnerable consumers. This includes 'age,' which implies young people would also enjoy some degree of protection. However, it is not made explicit how children and minors should be protected. Other EU consumer laws do not address children and minors at all, which could be considered a regulatory gap undermining coherence, when compared with other more recent EU laws where minors' protection is singularized and explicit. Academics have noted in relation to the UCPD that *"Where a commercial practice is specifically aimed at a particular group of consumers, such as children, it is desirable that the impact of the commercial practice is assessed from the perspective of the average member of that group. For this reason, the directive includes in the list of practices which are in all circumstances unfair a provision which, without imposing an outright ban on advertising directed at children, protects them from direct exhortations to purchase"*.⁴³⁷

The importance of international law should also be highlighted, as in recent years, this has influenced the development of EU law to protect children and minors who can in certain circumstances be vulnerable consumers.

The United Nations Convention on the Rights of the Child (UNCRC) is a legally-binding international agreement setting out the civil, political, economic, social and cultural rights of every child, regardless of their race, religion or abilities. The Treaty on European Union (TEU) set out the EU's obligation to promote the protection of the rights of the child under Article 3(3), which established the objective for the EU to promote protection of the rights of the child. The Charter of Fundamental Rights is also relevant as protects the rights of the child, including the child's right to privacy.⁴³⁸

There have also been voluntary initiatives to help promote children and minors' rights vis-à-vis advertising. On June 14, 2022, representatives of the EU's Consumer Protection Cooperation (CPC) Network, together with several national data protection authorities in the

⁴³⁷ The Regulation of Child Consumption in European Law: Rights, Market and New Perspectives (2009), Maria Luisa Chiarella, Facoltà di Giurisprudenza,

Università Magna Graecia (Catanzaro), https://indret.com/wp-content/themes/indret/pdf/655_en.pdf

⁴³⁸ Handbook on European law relating to the rights of the child (2022), FRA, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-2022-handbook-child-rights_en.pdf

EU and the secretariat of the European Data Protection Board (“EDPB”), endorsed five key principles for fair advertising to children. These are:

1. Take into account the specific vulnerabilities of children when designing advertising or marketing techniques that are likely to target children (in particular, do not deceive or unduly influence them, and consider whether certain types of personalized marketing are inappropriate for them altogether);
2. Do not exploit the age or credulity of children when engaged in marketing;
3. Explain to children, in a manner that is appropriate and clear to them, whenever general marketing content is addressed to them or is likely to be seen by them;
4. Do not target, urge or prompt children to purchase in-app or in-game content, and games marketed “for free” should not require in-app or in-game purchases to continue playing them in a “satisfactory manner”; and
5. Do not profile children for advertising purposes.

Some of these point to a blurring of the delineation between voluntary good practice principles and legislation. For instance, principle 2 “Do not exploit the age or credulity of children when engaged in marketing” is closely related to the UCPD definition in Art. 5(3). Principle 5 was already prohibited under the DSA’s Art. 28(2).

Some stakeholders such as children’s rights associations like the 5Rights Foundation have argued that the coherence of the EU legal framework – including EU consumer – could be improved if there were requirements where appropriate across digital and consumer law to ensure that traders in the digital environment design services from the outset that are child-friendly (and / or consider that some of their users may be users) for instance by designing age-appropriate interface design and/ or designing differentiated interfaces for children and minors. 5Rights notes that *“digital services that children and young people use are not designed to meet their needs or uphold their rights. Many services simply ignore the presence of child users (under 18s) altogether. Design decisions are driven more by the commercial requirement for data than by advanced consideration of a child’s best interests”*. 5Rights has produced various research reports to demonstrate that current legal provisions are often inadequate to protect children and minors given the absence of legal requirements in EU consumer law on digital fairness in online interfaces through compliance by design principles.⁴³⁹

They advocated that children’s safety, rights, and privacy are upheld by design and default. The GPSR provisions on child safety are a step forward in this direction, but focus on products, including digital products, rather than the full range of digital services, platforms and apps to address digital fairness.

The regulatory trend in addressing practices aimed at minors (e.g. in the DSA, GPSR, GDPR) also reflects the specific risks that children and minors face in the digital environment due to digital asymmetries, which are arguably more pronounced in the online world, requiring more specific rules to ensure adequate protection.

There is also arguably a need to improve coherence by updating EU consumer law to reflect improved attention to children and minors’ rights in the wide body of EU laws, to avoid consumer laws becoming outdated. In particular, the concept of a vulnerable consumer in the

⁴³⁹ See 5Rights report on [Pathways: How digital design puts children at risk](#) (on how specific design techniques, features and practices of digital products and services shape the experiences and behaviours of children and young people, based on interviews with both products/services designers and children as well as testing with avatars) and [Disrupted Childhood: the cost of persuasive design](#) (on the impact of such persuasive/behavioural design features on children’s social, mental and physical development).

UCPD needs to be clarified and an assessment made of how it is being applied in practice by traders and by courts. However, ensuring full coherence would imply going beyond definitions alone, and providing adequate protections e.g. considering compliance by design requirements for online interfaces, risk assessments to ensure age-appropriate design if users of digital services are likely to be minors or children, ensuring a reference to the need for traders to monitor manufacturers' compliance with the GPSR requirements relating to digital product safety, including cybersecurity and privacy.

Furthermore, more could be done to improve coherence in respect of rules concerning the use of children and minors' personal data for use in advertising and the prohibition of the profiling of minors for use in targeted ads. It is incoherent that this is already prohibited in the DSA, but not for all traders in the UCPD.

If EU consumer law were to be strengthened to improve coherence with EU and international law to improve protection of minors, some attention would be needed to ensuring an appropriate and uniform definition. In the UN Convention, a child is any human being below the age of 18 whereas, in national laws across the EU, there are differences in how a minor is legally defined.

3.5.14.3 Dark patterns

The findings in respect of dark patterns as a problematic practice were set out earlier in the report. However, the coherence of existing EU rules should also be considered. As a result of legislative activity in the past two years, dark patterns are regulated in many different pieces of EU law, such as the DSA, Data Act, AI Act and DMA, but also through the UCPD's general principles-based clauses. Some of the main pieces of law where dark patterns are now summarised (given that an exhaustive assessment would be too long).

Overall, the regulatory approach to addressing dark patterns is somewhat fragmented as many different pieces of EU legislation addressed dark patterns.

There is a challenge in ensuring a universal definition of dark patterns, but the DSA provided a definition in EU law for the first time. Nonetheless, it may be also argued that "dark pattern" describes a diverse and changing phenomenon that can be covered by different terms and legal concepts already provided for by existing laws. In that regard, a definition of dark pattern would not be essential, provided that existing rules cover them. For instance, the UCPD would not need to include the term dark pattern as such, provided that there is no obstacle in the rules prohibiting misleading actions or misleading omissions to embrace dark patterns. There are so alternative ways to achieve coherence in this regard.

The UCPD does not address dark patterns explicitly, but it is made clear in the 2021 Guidance that these are covered through the general principles-based provisions. For instance:

- Art. 6 prohibits deceptive practices that would deceive the average consumer (this implies coverage of deceptive design interfaces and practices such as drip pricing etc.);
- Art. 7 on misleading omissions bans hidden advertising and any dark patterns that involve hiding information;
- Art. 8-9 on aggressive practices cover coercive dark patterns such as 'confirm-shaming,' 'forced disclosure,' 'forced action and timing', 'forced continuity', 'nagging' (i.e. repeated nudging to ask consumers whether they want to upgrade and sign up for a paid-for service);
- Moreover, Annex 1 provides a blacklist of prohibited practices, some specific practices are outlined, such as point 7 which covers fake countdown timers to pressure customers to purchase a product by a fake deadline.

In the DSA, Art. 25(1) - Dark patterns in online interface design and organisation prohibits dark patterns. *“Online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates their users or in a way that otherwise materially distorts or impairs the ability of the users of their service to make free and informed decisions”*. Art. 25(2) states however that the provision in Art. 25(1) is not applicable “to practices covered by Directive 2005/29/EC or Regulation (EU) 2016/679” i.e. if the practices concerned are covered by the UCPD or the GDPR. This is seen as unclear, as has been flagged in consultation responses, interviews and as identified in the literature review. Because the UCPD is meant to provide a backstop, practically all commercial practices fall under the UCPD, therefore it is unclear which specific practices are left to fall under Art. 25(1) of the DSA. That leads to coherence problems, as when the DSA is applied to online platforms, UCPD can also apply based on personal scope (traders) and material scope (dark patterns amounting to unfair commercial practices). Lack coherence may emerge if the duplicated application leads to conflicting or uncertain consequences. But it is also caused by the uncertain and unclear implication of Art. 25(2) DSA.

The DMA prohibits "gatekeepers" from repeatedly soliciting consent through so-called nagging in Art. 5(2), a form of dark pattern. The DMA also prohibits dark patterns used by gatekeepers when those are deployed to circumvent the obligations in Articles 5, 6 and 7 DMA (Art. 13).

The GDPR also indirectly regulates dark patterns through various provisions, including those identified in the 2022 EDPB guidelines on deceptive design patterns, namely:

- The recitals of the GDPR outlines some important principles such as that consent should not be regarded as freely given if the subject has no genuine or free choice (Recital 42). This is then complemented by specific provisions.
- The processing of personal data (Art. 5). Lawfulness, fairness and transparency (Art. 5(1)(a) GDPR)
- Transparent information (Art. 12 GDPR)
- Accountability (Art. 5(2) GDPR)
- Data minimisation and purpose limitation (Art. 5(1)(b)–(c) GDPR)
- Data protection by design and by default (Art. 25 GDPR)
- Conditions for consent (Art. 4(11) and the conditions for consent for processing (Art. 7). Dark patterns such as requests for consent for data processing presented in an incomprehensible form or utilising subliminal techniques, are effectively banned by the GDPR.
- Provisions on the exercise of rights by data subjects (in particular, Art. 21 GDPR).

The Audiovisual Media Services Directive (AVMSD), as amended in 2018, provides additional requirements to the UCPD's general provisions regarding commercial communications, including some relevant to dark patterns, within its scope of application. The AVMSD bans deceptive audiovisual design, such as surreptitious advertising, subliminal techniques, and regulates the identification of sponsored programmes and product placement. The aim is to make viewers aware of being targeted with commercial ads such that they can make informed decisions. This addresses the problem of covert targeted ads through influencers that mix commercial and non-commercial content.

Dark patterns can also be sanctioned under competition law provisions. There have been legal cases involving the sanctioning of big tech's market dominance for positioning and displaying their own ads more favourably than competitors' ads, for instance on search engines. Any impeding of comparisons between services and use of default settings may also constitute

dark patterns that can be tackled under competition law.

The Data Act prevents data holders from making the exercise of choices or rights under this Article by the user unduly difficult, including by offering choices to the user in a non-neutral manner or by subverting or impairing the autonomy, decision-making or choices of the user via the structure, design, function or manner of operation of a user digital interface or a part thereof.

Whilst dark patterns are prohibited across different pieces of law, it should be stressed that the **scope varies between different pieces of law**.

Stakeholder feedback on coherence between EU consumer law and other laws in respect of the regulation of dark patterns is now considered, drawing on interviews and desk research.

Some interviewees, especially traders and their representative associations mentioned that it remains difficult to define dark patterns precisely. However, consumer associations pointed to progress in defining the problem of dark patterns in the DSA, alongside extensive public discourse and recent literature on problems relating to deceptive online design interfaces.

Whilst the DSA provides a more detailed definition of dark patterns, this is mainly focused on dark patterns in web interface design. There are perceived to be overlapping provisions between the DSA, UCPD and GDPR regarding dark patterns. Some legal academics interviewed commented that despite the *lex specialis* principle, the circumstances in which platforms should follow the specific rules on dark patterns in the DSA's Art. 25(1) given it is made clear in Art. 25(2) that if the practices are already covered under the UCPD and / or the GDPR, then those Directives should take precedence. This appeared incoherent to several legal academics and trader associations interviewed, leading to regulatory uncertainty. As it would mean that practices that strictly fall under Art. 25(1) are not then subject to UCPD and/or GDPR, but it is not clear why they are different and must be treated separately. Incoherence would lead to undesired effect if the standards applicable to such design practices under Art. 25(1) DSA would differ from those on which UCPD and GDPR are respectively based.

The same issue was identified in desk research:

“The DSA stipulates that it does not apply to practices covered by Directive 2005/29/EC or the GDPR, limiting the scope of its application and giving those acts priority (Art. 25(2) DSA). This means that if a given practice (dark pattern) of an online platform provider violates the GDPR, its legality will be assessed by the national data protection authority according to the requirements of the GDPR, not the DSA. Examples of such practices are included in EDPB Guidelines 3/2022.⁴⁴⁰ Similarly, if a practice violates national laws implementing the Unfair Commercial Practices Directive, those laws, enforced by the relevant consumer protection authorities, will apply. However, this framing of the DSA's interrelationship with the GDPR and Directive 2005/29/EC only theoretically solves the problem of overlap between these provisions in practice, as it is not always possible to unequivocally determine that a practice violates “only” the GDPR, “only” Directive 2005/29/EC, or “only” the DSA. Hence, it appears that parallel application of these laws in the digital sector will raise jurisdictional issues between national data protection authorities, consumer protection authorities, and digital service coordinators, and will require closer cooperation between them.”⁴⁴¹

Feedback on coherence in respect of EU rules on dark patterns was also received through the targeted survey. For instance, a national Ministry from Denmark commented that

⁴⁴⁰ European Data Protection Board "Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en

⁴⁴¹ "Dark patterns" targeted by EU institutions - Wardyński & Partners, <https://www.lexology.com/library/detail.aspx?q=cee82fe8-25c4-445d-9eaa-c747d1f0cc64>

considering the DSA's new rules⁴⁴², the UCPD should be updated to make it more fit for purpose in the digital age to address dark patterns, including through direct prohibitions in Annex I. For example, to ensure that the DSA and UCPD complement each other, we recommend that the UCPD's Articles 5, 6 and 7 should contain requirements for more visually and salient disclosure forms.

Some stakeholders view it as confusing that dark patterns are covered from many different perspectives in many different pieces of EU law. For example, the Norwegian Consumer Authority commented in their targeted response that Article 25 DSA has created uncertainty due to the overlapping nature between the UCPD and the GDPR in respect of dark patterns.

BEUC and other national consumer organisations and some legal academics supported the formal inclusion of a digital "fairness by design" provision, similar to the "compliance by design" provision in the DSA's Art. 31, supported by Art. 44 (voluntary) standards. This was viewed as potentially addressing the problem of dark patterns effectively. However, trader associations were concerned that this could risk undermining the technology-neutral asymmetry between the rules for online and offline. They advocated retaining the fairness test on a case-by-case basis.

Given deceptive digital design interfaces are a widely-discussed problem and that regulators globally are seeking to address the problem, it would improve coherence if dark patterns were explicitly referenced in consumer law, not only in the UCPD Guidance. For instance, Art. 8-9 UCPD on the use of harassment, coercion and undue influence appears to be outdated, as it does not refer to the digital environment, or the use of coercive practices that constitute dark patterns.

A 'compliance by design' clause could be introduced in the UCPD to mirror the DSA to improve coherence and address the dark patterns challenge from the outset of the interface design process. It should be considered whether this possible clause would be drafted as an obligation, that it is coherent in the DSA given its approach, or should be a prohibiting provision along the lines of the UCPD rules based on unfairness assessment.

Furthermore, the interplay between the rules on dark patterns in the UCPD and DSA should be made clear in the UCPD's recitals, not only in the DSA's Art 25(1) and (2). The Guidance should provide clear examples as to the circumstances in which online platforms' business practices should be subject to the DSA and when they should be subject to the UCPD. In addition, the relationship between the UCPD and other EU laws that address specific types of dark patterns could be explained in the UCPD Guidance, such as to make the inter-relationship clearer.

3.5.15 Overall findings

3.5.15.1 General findings – External coherence

Overall, **EU consumer law was found to be broadly coherent with other EU legislation** facilitated by mechanisms to ensure that inconsistencies and duplication are avoided, such as mentioning in the preamble and recitals and/ or in the legal provisions that the application of the legislation is *without prejudice* to other applicable EU laws, including EU consumer law; and considering that the UCPD's Art 3(2) and Art. 3(4) have been designed to secure that there are no conflicts between the generally-applicable rules in the UCPD and sectoral rules relating to unfair practices.

There is **growing regulatory complexity due to the inter-relationship between EU consumer law and different pieces of relevant legislation** that either some or all types of

⁴⁴² Under the DSA, large providers of online platforms must ensure that recipients of the service in a clear and unambiguous manner and in real time are able to identify whether the content is commercial (Art. 26 and corresponding Art. 44), including through prominent markings.

traders must apply in parallel. Examples are the DSA (platforms and marketplaces), DMA (gatekeepers, large online platforms and search engines), the AIA (developers of AI systems), the DCSD (digital service providers and content developers), the GDPR (all traders), the GPSR (all traders in non-harmonised sectors) and the AVMSD (audiovisual sector, including influencers).

Moreover, **similar regulatory challenges and objectives are tackled in different pieces of EU law but from different perspectives** (e.g. dark patterns, transparency of advertising, access to, and sharing of personal data).

Many pieces of relevant EU legislation to protect consumers and ensure digital fairness such as digital and data laws, were **either introduced or updated very recently**. These new pieces of law (e.g. DSA and DMA, AI Act, Data Act) and revisions of existing laws (e.g. GPSR, AVMSD, integration of provisions from the DMSFD into the CRD) were developed in response to developments in digital markets and services and which required strengthening of sectoral and horizontal consumer protection rules across different particular areas of the digital environment, for different types of traders and sometimes also to regulate specific business practices for digital transactions.

In contrast, despite progress in updating the underlying legal framework through regulatory amendments made by the MD, **most provisions in EU consumer law were developed a considerable time ago**, especially the UCPD and UCTD. A challenge in their application is that these Directives follow the general principles-based approach, whereas the trend in other EU legislation has been towards introducing more specific rules at least for some digital practices, digital services and content. This raises challenges in optimising coherence, according to some trader associations and legal academics as different types of law have evolved in different contexts, whereas **achieving digital fairness in EU consumer law requires closer integration in the design, drafting, interpretation, and application of EU consumer, digital and data laws**.

Accordingly, some stakeholders, especially consumer associations and legal academics, perceived that **more could be done to align, update and modernise EU consumer law with other recent regulatory developments to strengthen coherence and fitness for purpose of the EU consumer law framework in the digital age**.

Whilst there is only **limited evidence of legal incoherence in the strict sense**, there is a difference between a legalistic assessment of external coherence (to check any conflicting provisions, eliminate unnecessary duplication, identify outdated provisions due to new legal requirements in other legislation, gaps) and perceptions of coherence among stakeholders. For instance, some stakeholders noted that dark patterns and influencer marketing are covered from different perspectives in many different pieces of EU law, but with no single set of rules in a single piece of law, making it difficult for traders and other stakeholders to understand. The perception of multiplicity or fragmentation that may lead to the sense of incoherence is aggravated by the lack of a definition as such of these phenomena. They must therefore be addressed by subsuming the market practices in legal concepts and rules not explicitly addressing them. That does not mean that a legal definition is necessary, as the resultant risk could be that the definition becomes outdated.

The **positive and important role of Commission Guidance** in strengthening understanding among all stakeholders as to how EU consumer law should be applied in conjunction with other pieces of EU law should be highlighted. For instance, the UCPD Guidance was updated in December 2021 and includes a chapter on the "Interplay between the Directive and other EU law".

The relationship between EU consumer law, digital and data protection law in the EU could be made clearer. The presence of explicit rules on certain types of traders in terms of information disclosure and transparency requirements and/ or the prohibition of some

practices in conducting digital transactions in other types of EU law but not explicitly in EU consumer law is linked to the general principles approach. Unfair, misleading, and aggressive digital practices are already covered in a generic sense, it is a question of whether this is sufficient to provide coherence given many other pieces of EU law now include more specific rules for traders in the digital environment. The merits of general clauses though are this “closes” and maintains the completeness of the legal system, as they cover any practice that is not explicitly set out (e.g. through guidance).

External coherence can also be **impacted by wider market and technological developments**, as these have led to the adoption of new, and the revision of other existing EU legislation, which in turn has had implications for consumer law.

Lastly, the **forward-looking dimension to coherence** should also be considered. There is an issue as to how far EU consumer law and other types of laws will need to address further new and emerging developments in digital markets and services not yet reflected in EU law where regulation may arise in future (e.g. generative AI, growing use of virtual assistants and other intermediary services which are impacting the traditional relationship between traders and consumers).

3.5.15.2 Means of updating the legal framework to become more coherent

Regarding specific ways in which the consumer law framework could be updated, detailed suggestions are made in the legislation-specific and thematic sections presented earlier. In summary:

- Given the vital role of data in the digital economy, **there are coherence issues regarding whether EU consumer law rules should also include data protection rules directly**, or given that these are already covered in horizontal laws, instead signpost to relevant provisions in other EU legislation (notably the GDPR) to improve coherence. **Personal data** should be explicitly mentioned in all EU consumer laws and a definition should be included aligned with relevant EU data laws, especially the GDPR. The UCPD should provide more detailed provisions explaining the interaction between EU consumer law and data laws.
 - Profiling of sensitive data should be prohibited for all traders in the context of the UCPD, mirroring Art. 9(1) of GDPR and the DSA’s Art. 26(3).
 - Profiling of minors’ data for targeted ads should be prohibited as per the DSA’s Art. 28.
 - To improve coherence with the new GPSR, the importance of risk assessment by marketplaces to ensure that the personal data of minors is secure when using digital services not only digital products could be considered.
- The importance of consumers having access to their data could be explicitly mentioned, as means of accessing data subjects’ own data are already made clear in the GDPR (and in the Data Act), and the portability and use of user-generated non-personal data has been tackled in the Data Act. The extent to which extending such rights to consumers for personal data would be beneficial should be explored to strengthen coherence in the treatment of data in consumer law with other relevant data laws.
- Incoherence was identified in the interaction between the DSA and the UCPD on dark patterns as specified in Art. 25(1) and Art. 25 (2). Whilst *lex specialis* is meant to be applicable, the provision in Art. 25 (2) that if (unfair) practices are already covered by the UCPD or GDPR these Directives should be followed was seen as unclear and

contradictory. This was raised in the public consultation⁴⁴³ and targeted consultation responses, academic literature and in interviews. Therefore, this lack of coherence should be addressed and it should be made clearer which types of unfair practices fall under the DSA for platforms and those practices that fall under the UCPD for the traders that must follow both sets of rules. More concerning would be that the standard to assess the practices under Art. 25(1) DSA and the practices falling under UCPD and/or GDPR might be deemed to differ. If so, incoherence would lead to differentiated treatment in analogous practices.

- Given the focus in other recent new and updates of existing EU legislation (and in competition law) on ensuring that consumer choice is not limited, a **provision on ensuring digital fairness by design from the outset should be considered. Dark patterns** are explicitly regulated in many other pieces of EU law and whilst they are also covered in the UCPD, arguably insufficiently clearly. Linked to this, compliance by design in online interfaces should be considered as a means of strengthening the overall coherence and effectiveness of the consumer law framework.
- **The protection of children** should be strengthened, as there are relevant provisions specific to the digital environment in other relevant EU legislation which recognises children's specific vulnerabilities.
- **Influencer marketing** could be mentioned in EU consumer law or even subject to specific rules. This could be helpful in consolidating different rules across different pieces of EU law as there are no specific targeted rules applicable to influencers. Currently, influencer marketing is not explicitly mentioned in the UCPD, but is covered through several of the general principles-based provisions, including through a focus on misleading omissions in relation to hidden ads. This is not incoherent compared with other EU laws, which also regulate hidden ads and commercial content.⁴⁴⁴ However, this would require a definition of an influencer which may create further complexities and incoherences.
- In line with the general principle included in some EU laws (e.g. the DMA) and in the UCPD Guidance that it should be easy to exit as to enter into a contract, the CRD has newly incorporated a right of withdrawal button (because of the regulatory amendments made in respect of distance contracts in financial services). From a coherence perspective, applying this principle - subject to any stipulated cancellation periods - should ideally be applied in all relevant EU legislation to ensure that consumers are better protected from subscription traps.
- The **possibility of a mandatory cancellation button** should therefore be considered. This would need to ensure sufficient flexibility as to how this might be applied across different types of digital market and services, such as websites, apps, and platforms, as it should be as technology-neutral as possible. It does not have to be a button per se but a means of cancelling a contract easily (e.g. it could also be via the settings or account details in an app).
- **The right to a human interlocutor was introduced through the recent 2023 Distance Marketing in Financial Services Directive.** The CRD previously focused

⁴⁴³ See for instance the public consultation position paper submitted by ELI, the response on the Need for Stronger Protection Against Unfair Digital Practices (Q1) which refers to the unclear relationship between the UCPD and the DSA, especially on dark patterns
https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Response_of_the_ELI_to_the_European_Commission's_Public_Consultation_on_Digital_Fairness_.pdf

⁴⁴⁴ The interaction between the UCPD and other EU laws relating to influencer marketing is not incoherent, as other legislation provides more detailed rules in particular areas, and the *lex specialis* principle is applicable. However, there is a debate considered earlier in the report as to whether dedicated EU rules could be needed within EU consumer law to avoid the emergence of national regulations on influencer marketing, which could undermine coherence and effectiveness.

on other communication means, such as ensuring access to a standard rate phone number. However, interacting with traders via a chatbot has become more common than making a phone call in many areas of digital services, such as the online travel sector, airline ticket bookings etc. This right could be extended to all sectors within the CRD. To a certain extent and within the scope of the provision, Art. 22 GDPR is connected with this right to obtain human intervention. Coherence on the extent and the meaning of the right and the situations covered is desirable across EU laws.

3.6 EU added value

According to the Better Regulation Guidelines, an evaluation should consider arguments about the additional added value from EU interventions in the fitness check context, we have assessed how far the consumer law framework has added value from a digital fairness perspective in preventing unfair contract terms and ensuring greater transparency in contract terms, and prevented unfair commercial practices and distance contracts.

The situation that would have resulted in a counterfactual situation in which there was no EU regulatory framework and only 27 different national sets of rules was analysed, including the impact of the lack of a Digital Single Market dimension.

EQ18 – What is the overall EU added value of the EU consumer law within scope in the context of digital fairness?

- The UCPD, UCTD and CRD have delivered EU added value by providing a stable regulatory framework over an extended period since the early 1990s (UCTD, 1993), with the progressive accretion of additional consumer laws (UCPD, 2005, CRD 2011). This was appreciated by consumers and traders alike as having added value by providing an EU-level legal framework whereas prior to the existence of EU consumer law, there were many different national consumer law frameworks.
- Added value is arguably incremental over time, as the EU has increased in size e.g. due to EU enlargement processes. However, the growth in digital markets and services occurred mainly after EU enlargement and therefore the digital fairness dimension has added value across all EU-27 MS.
- The UCPD's role in providing consumer protection as a fallback when no specific alternative sectoral legislation is applicable was valued by consumers and their representative association.
- The Directives' technology-neutral nature has added value through the general principles-based approach without the need for more specific rules, as the Guidance has been updated in a way that explains the implications of the existing rules for new and emerging business practices. This has helped to achieve digital fairness.
- However, rapid developments in other areas of EU law, especially digital and data-related laws may underline the ongoing ability of the legislation to deliver digital fairness without further regulatory alignment and modernisation. More detailed rules in a few areas could arguably provide greater regulatory certainty allowing EU consumer law to continue to add value through its positive role in ensuring high levels of consumer protection.

EU consumer law was perceived as having added value by ensuring an effectively-functioning single market. In the context of this study, it was viewed by trader associations as having:

- Delivered a Digital Single Market whilst ensuring protection for consumers.
- Delivered regulatory stability, through the application of a general principles-based

approach in conjunction with the role of national case law and the updating of Commission guidance on the Directives' application in the digital age. Traders viewed these features of the way the application of the legal framework works as having helped to accommodate technological changes, developments in digitalisation in the European and global economy and the rapid growth in digital markets and services, and the development of new business practices within these markets.

Among consumer associations, CPAs, Ministries and legal academics, the consumer law legal framework was viewed as having delivered the above benefits. However, there were concerns that whereas historically, the updating of the guidance and general provisions have allowed the UCPD and the UCTD to accommodate new developments, the pace of regulatory and technological changes has increased. Therefore, there was a perception that the consumer law framework if there is no further adaptation and modernisation may no longer be able to add as much value in future years as it has in the previous 20 years (unfair commercial practices) and 30 years (unfair contract terms). Stakeholders representing the consumer and the trader perspective acknowledged that whereas EU consumer law has added value over a lengthy period, in the past few years, the pace of regulatory change has accelerated in EU consumer law, through the 2019 adoption of the Modernisation Directive and regulatory amendments to the underlying legislation within scope (e.g. the UPCD, UCTD and CRD). In addition, rapid developments in other relevant EU legislation where there is a close interaction with EU consumer law, such as digital and data laws has evolved.

Considerable EU regulatory developments have taken place in areas of law applicable in close conjunction with consumer law, especially digital and data laws (see external coherence in sections 3.6-3.9) raise considerations as to how well-equipped the EU consumer law acquis is to deal with comparatively new challenges, such as applying and enforcing consumer law in conjunction with data law and testing the fairness of data exploitation strategies, when these involve the application of the UCPD, UCTD and GDPR in parallel.

Examples of more specific feedback on the EU value added of EU consumer law were identified. BEUC attested to the benefit of having the UCPD that it provides a consumer protection fall-back option to ensure that wherever there is no sectoral legislation, consumers remain protected.

An EU industry association focusing on the data side of marketing advocated that regulators and consumer associations should work in close conjunction with industry to ensure that EU consumer law continues to add value when applied in conjunction with other EU laws in the digital environment, and by including additional examples of how to apply different business practices in a compliant way with existing legislation.

“Further guidance has the potential to bring significant added value to the implementation of existing legislation in the digital environment. To ensure the pragmatic applicability of further guidance, the European Commission or any other competent authorities should seek input from businesses. It is also important that on topics that are also covered by other pieces of legislation (for instance processing of data, use of AI, dark patterns...), the Commission works with relevant regulators and other Commission’s Units to align positions and avoid fragmentation of interpretations.”

A large trader in the global tech industry expressed concerns regarding the risk that EU added value from the maximum harmonisation character of the UCPD risks being undermined by regulatory fragmentation at national level covering influencers (FR) and the cancellation button (DE). The lack of clarity at EU level as to whether similar requirements will be introduced in future and the current regulatory fragmentation at national level was seen as undermining the value added of consumer law in a digital context.

Overall, EU consumer law was perceived as having added significant value. However, achieving digital fairness has grown more challenging and complex considering technological/

digitalisation-related alongside market-driven and regulatory developments. Therefore, without some further streamlining of the legal framework to provide additional regulatory certainty in specific areas, such as dark patterns and subscription traps, some stakeholders perceived there as being limits as to how far the existing consumer law framework can add as much value in future as it has in the past 20-30 years without further updating.

EQ19 What would have happened in the absence of regulatory intervention through EU consumer law at EU level to ensure (digital) fairness?

This EQ considers the counterfactual i.e. what would have been the situation if the UCTD, UCPD and the CRD had not existed (or were to be repealed in future). In the Better Regulation Guidelines, consideration of the counterfactual is emphasised as a means of testing what value added EU law has brought, by considering alternative scenarios in which such legislation did not exist.

Without EU consumer law, according to stakeholder feedback, there would have been:

- 1. Member States would have had to regulate unfair commercial practices and contract terms, and consumer protection aspects of distance contracts through national rules, with divergence in national rules.** There would have been 27 different national regimes, with regulatory fragmentation. MS would have had to develop and implement their own rules to ensure high levels of consumer protection. National rules have already begun to diverge in certain areas to regulate specific business practices and / or types of traders in the digital environment, despite the UCPD being a maximum harmonisation Directive. The situation is likely to have been worse were it not for the existence of EU consumer laws.
- 2. A missed opportunity for the Digital Single Market (DSM) given the high costs of “non-Europe”.** The potential benefits for the DSM of an EU consumer law framework, with harmonised rules and a stable regulatory regime would be diminished. These would be less cross-border trade and consumer trust and confidence in conducting transactions in the digital environment cross-border would be eroded as consumer rights when purchasing from other countries would vary and be more difficult to enforce.
- 3. Consumer protection would be diminished.** There would be greater difficulties for consumers in navigating different rules across different EU countries and it would be more difficult to make complaints and to pursue or to obtain redress.
- 4. A damaging effect on consumer trust in the absence of EU consumer laws providing a regulatory backstop through general consumer protection rules** in cases where no specific sectoral rules exist.
- 5. Reluctance among consumers to conduct transactions in the digital environment, especially on a cross-border basis.** Therefore, the impact on market size of not having any EU-wide consumer rules might be in the region of 10%. Without such rules, there would likely have been lower levels of trust and confidence among consumers (as monitored through the CCS) and less willingness to engage in transactions online for digital goods and services.

Whilst the EU added value of EU consumer law is difficult to quantify, it can be asserted that the increased size of the European digital economy, which has grown markedly in the past decade means that the role of consumer law has played an important role in creating the necessary regulatory framework conditions for the development of a single market in digital markets and services. As explained in Section 3.2.2 (development in B2C digital markets and services), e-commerce was estimated to be worth EUR 626 billion / year in 2023, with the

European platform economy estimated to be worth EUR 14 billion / year (2020), and the European subscription economy a further EUR 129 billion / year (2022). If no DSM existed, underpinned by consumer law to protect consumers, the market size would arguably be less, even if it is difficult to assess the precise impact due to the absence of EU consumer law within the single market.

In the absence of the UCPD, according to BEUC, consumers would have to fall back to national tort law as the means of ensuring consumer protection, where the evidentiary requirements to prove harm are significantly higher.

EQ20 – How can market practices be expected to evolve and what would be the most likely consequences if there is no further strengthening of the Directives with respect to consumer protection in the digital environment?

Market practices continually evolve, due to the rapid evolution in digital markets and services and developments in new technologies and the ongoing impacts of digitalisation across different sectors within the digital environment (and offline sectors moving partially online in a multichannel context). This was demonstrated in the extensive assessment of market practices and their evolution in Section 2 on problematic practices and in the case studies. The expected evolution in business practices is also linked to EQ10. Moreover, the periodic updating of the guidance on the application of the UCPD, UCTD and CRD demonstrates that practices evolve and there is a need for updating of guidance accordingly, which is why, for instance, the UCPD guidance includes a chapter on the Directive's application in a digital context, which explains prohibited practices and how traders can ensure compliance with existing requirements across different practices.

It is **difficult to predict how market practices will evolve and which types of practices may emerge in future**. Digital markets and services are inherently dynamic and innovative and have evolved rapidly. Key trends that can be observed which influence business practices are: the growth in **online subscriptions** and the **platform economy**, the growth of the **European gaming industry** and the ever-growing importance of **AI systems and algorithms** which are central to the functioning of search engines, platforms, and marketplaces. Further trends are already emerging, for instance increased use of **generative AI**, and other trends may take off and soon become mainstream, such as the **metaverse**. For the size of these markets, refer to section 3.2.2, which considers current developments in the evolution of B2C digital markets and services.

Data-driven personalisation practices and the growing use of consumers' personal data and of their non-personal data for big data analytics are at the core of many digital economy business models. Regular use of online services to communicate, inform oneself and purchase products and services generate large amount of data, which can be used to infer information about consumers. In the past, the use of data driven practices was the remit of large companies. With the development of new analytics tools and automated decision-making processes, smaller operations are now capable of using data-driven practices. Some data-driven personalisation practices such as personalised rankings, personalised advertising of personalised communications are seen by industry as legitimate and benefiting the consumer, and is considered crucial to many traders' business models in the digital environment. Personalisation and the data-driven internet is the main income stream for large social media platforms.

However, there are challenges regarding the growing use of personal and non-personal data in a consumer protection context, such as the fact that EU consumer law does not generally deal directly with data (including the issue of sensitive data), whilst such issues are dealt with in digital and data laws. The extent to which there are any legal gaps resulting from the development of different laws that must be applied in parallel is dealt with in the external coherence section. An observation in terms of how far data-driven business practices require

strengthening of the Directives is this depends on different stakeholder viewpoints on the optimal regulatory architecture. Some stakeholders argued for instance that it is not necessary to update consumer law to reflect the growing tendency towards data-driven business practices for “free” digital services as traders must apply the GDPR which already provides protections around the use of sensitive data, the need for traders (as data processors) to specify a legitimate rationale and business use for the collection of personal data. However, other stakeholders perceive that as per the DSA approach, it would be better to codify some of the provisions that affect business practices directly into consumer law to avoid regulatory uncertainty and to make the provisions clearer, given that personalisation practices have become ubiquitous. The Commission’s guidance clarifies that the UCPD, as well as other pieces of legislation including the ePrivacy Directive, the GDPR or sector-specific legislation “can be used to address unfair data-driven business-to-consumer commercial practices”.⁴⁴⁵ The UCPD could in theory already cover many different new and emerging business practices, such as those linked to the use of AI, algorithms, and automated decision-making, as these must still avoid unfairness according to the general principles-based provisions. Reference should be made to the more detailed assessment in EQ10 on the impact of new technologies and digitalisation on the legal framework’s ongoing effectiveness.

A technology foresight approach could be used to monitor technological and digitalisation-related developments and to consider how this may influence traders in terms of their business practices. For instance, wider use of generative AI raises a whole series of consumer protection issues, as considered earlier in the EQ on new technologies and their impacts and as observed by the Norwegian Consumer Council in their report on the impacts of AI for consumer protection.⁴⁴⁶ Generative AI tools are being integrated into products, online platforms, search engines and / or within websites to provide information to support consumers. There are already provisions within the UCPD that if information provided is misleading or deceptive and influences consumers into taking transactional decisions they would not otherwise have taken, this would be deemed unfair under the general fairness test. However, caution is needed in assuming that the existing legal framework could cope with all aspects. For instance, whereas the MD recently introduced in the CRD a requirement that platforms must inform consumers regarding personalised pricing based on automated decision-making, there could be challenges concerning the interpretation of such a clause when human and automated decision-making was combined.

Furthermore, it is not just digital markets and technologies that are dynamic, but also the concept of a trader, and the types of services they offer. Not only are business practices regularly evolving, but the concept of a ‘trader’ is becoming more complex, with a growing trend for an **increasing number of roles taken by some actors**. For instance, online platforms have moved beyond providing digital services in exchange for consumers accepting personalised advertising, and have moved into other markets, such as offering premium subscriptions and increasingly entering the marketplace area by facilitating direct sales to consumers. As such, there may be a need to clarify roles and responsibilities to ensure that the practices that platforms playing more than one role are adequately covered.

Moreover, the role of different economic operators with the supply chain should be noted. Whereas the New Legislative Framework (NLF) focuses on the concept of economic operators, EU consumer law legislates the business practices of traders. However, **not all economic operators in the supply chain with an impact on consumer protection in the digital environment are presently dealt with in EU consumer law**. Consumer law regulates the traditional relationship between traders and consumers, but does not specifically regulate other actors within the supply chain, for instance, website designers and UX developers

⁴⁴⁵ 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, p 99.

⁴⁴⁶ Ghost in the machine – Addressing the consumer harms of generative (2023), AI <https://storage02.forbrukerradet.no/media/2023/06/generative-ai-rapport-2023.pdf>

working on design interfaces for platforms, or intermediaries that play an intermediation role between traders and consumers, such as recommendation services. Whilst EU consumer law focuses on B2C relationships, it should be recalled that there are B2B relationships between third parties and traders in a digital context that affect the application of EU consumer law. For instance, traders may work with third parties that design online design interfaces, be these websites or platforms. An authority in the Netherlands noted in their targeted position paper the *"absence of legal responsibility for some of the players in the B2B chains that produce those harmful designs"*.

The principle of technology-neutrality underpinning the legal framework has largely sufficed so far in ensuring that new technologies and trends are still covered by the existing framework. However, some stakeholders, including consumer associations and Ministries in charge of enforcement saw the need to clarify and strengthen certain rules in the digital environment to ensure a greater level of certainty. There is a risk of **legal gaps emerging if the legal framework specific to consumer protection is not reviewed, updated, and modernised** (see Section 3.5 (external coherence)). Most of the experts consulted during the study considered that data-driven personalisation practices are more problematic than classic dark patterns, especially as they are more difficult to identify and investigate due to individual personalisation and group segmentation based on the use of personal data but the detailed configuration of data being used is not clear to CPAs, which makes investigating the fairness of the use of such data difficult to investigate (see EQ5 on enforcement).⁴⁴⁷ With the increased use of data driven techniques by a wider array of companies, including SMEs, there is a risk that the current legal framework may be too vague to capture the specificities of the practice.

Overall, the likely consequences if there is no further strengthening of the Directives with respect to consumer protection in the digital environment are:

- The **effective application of the current EU consumer law acquis** would continue to rely upon the general principles-based approach and the regular updating of guidance in combination with national case law. This approach is tenable to a degree and supported by many traders and trader associations.
- However, there **could be some potential disadvantages of relying on the status quo approach to regulating B2C transactions in digital markets and services**. These could limit the consumer law regime's added value in future. Examples are:
 - Slow pace of change when relying upon national case law and CJEU rulings to clarify whether new business practices are unfair, deceptive or aggressive. These often takes years to emerge.
 - Lack of clarity as to the obligations of specific types of traders involved in business-to-consumer (B2C) practices. The current legal framework defines a trader, but does provide definitions of some of the different types of traders prevalent in the digital environment.
 - Absence of legal certainty as to which practices are prohibited, and which are regulated and what the rules are. With the increasing availability of more complex and potentially manipulative techniques, there is a need to clarify which practices are allowed and which ones should be banned. A lack of action is likely to allow problematic practice to continue.
 - Difficulty in addressing digital asymmetries. Consumers are less able to make informed choices in the digital environment partly due to information asymmetries, but also due to design choice architectures and online interfaces.

⁴⁴⁷ European Commission (2022). Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation, available at: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>

4 Summary of Fitness Check findings and conclusions

The overall findings and recommendations from the fitness check are now set out. The findings are structured by evaluation criterion and draw on the evidence base from the desk research and stakeholder consultations that have taken place, with triangulation of primary and secondary data and information sources (e.g. the interview programme, public consultation, consumer survey, enterprise survey and targeted survey and sweeps).

4.1 Overall findings

4.1.1 Effectiveness

Overall, good progress has been made through the application of EU consumer law towards the achievement of the objectives of high levels of consumer protection (including in the digital environment) and a better functioning of the internal market through harmonised rules. However, challenges remain, meaning that the legal framework and its effective application is not yet optimal.

Challenges include the **proliferation of problematic business practices in the digital environment**, the existence of **legal uncertainty** in certain areas, combined with the **absence of specific rules given the rapid advances in the development of digital markets**. Weaknesses in the **private and public enforcement of consumer law** in the digital environment were also identified.

There was a consensus among stakeholders that the **general principles-based approach** established in the UCPD and UCTD has been an important factor in ensuring their effectiveness over the years. This approach is non-prescriptive and can **generally accommodate new technologies and changes in business practices**, with the updating of guidance providing illustrations of how to address new and emerging business practices in EU consumer law, and/ or making clear which practices are prohibited. However, **case law takes considerable time to emerge, whereas business practices evolve rapidly and give rise to unfair commercial practices and unfair contract terms**. For instance, terms and conditions identified as unfair may have gone through numerous changes by the time enforcement cases reach an outcome. Moreover, compared with offline transactions, there is a comparative lack of case law, meaning that legal uncertainties do not get clarified within a reasonable timescale compared with the pace at which digital markets and services develop.

Furthermore, **technology-neutrality** and **sales channel-neutrality** were strongly supported, especially by trade associations. However, other stakeholders such as consumer associations, Ministries, CPAs, and legal academics favoured more specific rules in certain areas, citing greater asymmetries faced by consumers in the digital environment versus offline. Despite EU consumers being more willing to conduct transactions in the digital environment than when the 2017 fitness check was conducted,⁴⁴⁸ consumers nonetheless continue to encounter problems in exercising their rights in the digital environment. This undermines the objective of high levels of consumer protection (see Section 2.1 on the pervasiveness of problematic practices and for survey data on individual problematic practices).

For instance, in the public consultation survey, on average, 31.4% of consumers had a problem three times or more per year, and 28.3% once or twice per year. In the consumer survey (10,000 consumers), on average, in the past year, 50.3% of consumers experienced

⁴⁴⁸ Data from the Consumer Conditions Scoreboard 2023 (and its predecessors) that EU consumers are more willing to conduct transactions online than years ago (circa + 15 pp. in 2023 compared with 2016 data the previous fitness check used, as digitalisation has become more pervasive across the EU-27.

situations of problematic practices when purchasing a product or services online, including digital content/services/subscriptions. Among these consumers, 6.2% reported that they always experience such situations, 16.1% say that they experience them most of the time and 28.0% experience them sometimes.

While acknowledging the regulatory certainty provided by the long-standing legal framework, stakeholders highlighted the existence of considerable **legal uncertainty about the application of EU consumer law in the digital area**. In the public consultation, 52.0% 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. 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 (54.0% strongly agree, 29.0% agree). Although some of the problematic practices could be tackled, in theory, by the existing rules, they nevertheless remain persistent. This suggests ongoing challenges with public and private enforcement, but also a need to increase levels of awareness among traders regarding the existing legal framework and their obligations. Some practices that have long been prohibited, such as hidden advertising (UCPD), pose new compliance challenges when implemented in the digital environment, for example with social media influencers. It is questionable whether the current rules provide sufficient legal clarity or are adequately well-known and understood by traders.

Furthermore, the **emergence of national and international legislation** with more specific rules on problematic practices creates issues of **regulatory fragmentation** and **undermines the effectiveness of the current rules**, considering the maximum harmonisation nature of the UCPD and the CRD. Divergences in national rules, guidelines and case law were observed, among other areas, on dark patterns, influencer marketing, subscription traps, loot boxes, and more broadly concerning the protection of minors. **Action at EU level may be necessary to avoid the emergence of a patchwork of new national legislation**, which are covered through the UCPD's general provisions and definition of vulnerable consumers, albeit insufficiently, according to some consumer associations, CPAs, and Ministries.

The **Modernisation Directive's application has helped to strengthen the fitness for purpose** of the three Directives within scope. This has contributed to strengthening effectiveness, for instance through greater transparency for consumers due to new disclosure requirements for platforms and marketplaces (e.g. fake reviews, transparency of search rankings, whether sellers are professional traders or an individual). However, the sweeps revealed that **adequate trader compliance with some of the new requirements is still lacking**. The MD has also made a valuable contribution to strengthening enforcement and providing redress possibilities, especially through more **harmonised penalties for certain cross-border cases**, and a stronger deterrent effect through **higher penalties for repeated infringements**.

There was a consensus that whilst there have been improvements in enforcing the existing consumer law framework, **enforcement remains a weak point in its effective application**. Although some positives can be noted (e.g. greater cooperation between CPAs through the role of the updated CPC Regulation and harmonisation in penalties through the MD), activity levels in enforcement appear to vary between different CPAs. Whereas some CPAs have expertise in enforcing EU consumer law in the digital environment, others were found to lack such experience. This suggests a need for **further capacity-building, but also promoting good practices in enforcement in the digital environment**, such as setting up a division within a CPA dedicated to digital cases to reflect their added complexity and the frequent inter-relationship between EU consumer, data and digital laws and using digital means, including automation (such as web crawlers) to automatically check compliance. Whereas some CPAs have taken on complex strategic deterrent cases against major players in the digital environment, others have not done so. Enforcement is increasingly complicated due to the

additional complexity of applying EU consumer law in concert with other digital and data laws, which requires further resources and knowledge. This has led to **fewer enforcement actions in digital contexts** than has historically been the case offline.⁴⁴⁹ Furthermore, there have been **comparatively few examples of national case law in the digital area**, leading to delays in the process of jurisprudence providing regulatory certainty. Whilst problematic practices already covered in EU consumer law can be clarified through case law and CJEU rulings, **strengthening regulatory clarity in the face of new and emerging business practices through jurisprudence takes a lot of time**.

CPAs need to strengthen their capacity to take on enforcement cases as a strategic deterrent to non-compliant traders, including by developing improved skills in-house to proceed with enforcement cases in the digital environment and using digital tools to widen the number of compliance checks performed in the digital age. Additionally, **CPAs need to exercise their existing regulatory powers under the CPC Regulation where necessary**, such as compelling traders to provide evidence. This could be used, for instance, to request that traders explain features of design interfaces where complaints have been received and it would otherwise be difficult for CPAs to investigate digital fairness without input from the trader due to information and technological asymmetries (e.g. investigating the fairness of an algorithm). To address the complex challenges of price discrimination, deceptive choice architectures, and biases inherent in AI systems, CPAs need to significantly 'tool up'. Furthermore, there is a need for closer cooperation between CPAs, data protection authorities and competition authorities.

Whilst penalties have been harmonised through the transposition of the MD, there **remain challenges in ensuring a harmonised approach as different CPAs adopt different practices in using their enforcement powers to impose fines**, resulting in an unevenness between different MS in the fines being issued. However, assessing the full impact of the harmonisation of penalties in the MD would at this stage be premature, as the effects will take time to fully manifest. The global nature of digital markets and services, with some market players having a considerable market share and operating on a pan-European basis raises the issue as to **whether the EU should play a role in ensuring a more harmonised approach to enforcement and issuing penalties for non-compliance with consumer protection rules**. The need for an increased enforcement role for the Commission was flagged by some of the stakeholders, to mirror the regulatory approach in the DSA and DMA.

Overall, **EU consumer law has made a positive contribution to achieving digital fairness**, which was found to be implicitly linked to delivering the regulatory objective of achieving high levels of consumer protection through the implementation of the UCPD, UCTD and CRD. However, many stakeholders were concerned that the current framework is sub-optimal for consumers due to digital asymmetries that challenge the foundations of the current EU consumer law approach to regulating the business-consumer relationship. As far as the way ahead is concerned, stakeholders held diverging views. Many trader associations favoured improved enforcement combined with the regular updating of the supporting Commission guidance on each of the Directives as a more effective means of improving consumer protection than further EU rules. In contrast, consumer representatives, some national Ministries, CPAs and legal academics favoured introducing at least some more specific rules to strengthen regulatory clarity and ensure the continued effective functioning of the legal framework.

4.1.2 Efficiency

The EU consumer law framework within scope has been **efficient overall**. The compliance costs were found to be reasonable and proportionate given the importance of achieving the

⁴⁴⁹ As an example, there were found to be numerous price promotion cases involving offline whereas there are only a couple of cases involving price promotions online, though more may emerge due to the new rules on av. price promotions in the PID.

objectives of high levels of consumer protection and a harmonised single market. There was found to be a **positive relationship between benefits and costs**, though benefits were difficult to monetise. The total administrative costs of checking compliance have been estimated to be in the range of EUR 249.8m to EUR 487.5m. The costs of information disclosure (information obligation) were found to be negligible. Adjustment costs have been estimated to be in the range of EUR 208m to EUR 303m across the EU.

The **recurring costs have been kept relatively modest**, since the core legislation has provided **regulatory stability for a long period of time**, supported by the periodic updating of guidance. However, the degree of stability has lessened in recent years, due to developments in new technologies and digital markets, and major developments across the EU legal framework, especially through digital and data laws, but also in other areas of EU legislation beyond consumer law. Whilst some traders incurred compliance costs because of recent changes to consumer law through the MD, which amended the underlying legislation, most traders viewed the changes specific to the digital environment, such as requiring additional information disclosures on platforms, as not being that onerous, at least after initial familiarisation costs.

The main benefits identified by traders included facilitating trade within the digital single market and reducing **barriers to cross-border digital trade through the maximum harmonisation approach of the UCPD and the CRD** being applied in the digital environment. However, the blacklist in the UCPD, which includes only a limited number of prohibited practices that are digital-specific, could be further strengthened to ensure a more level playing field for traders (recognising that many traders actively invest to comply with EU consumer law) and the introduction of a blacklist in the UCTD was suggested.

The main benefit for consumers is the **promotion of digital fairness and protection from unfair practices and unfair contract terms**, although this is not presently optimal due to the ongoing presence of digital asymmetries, a lack of digital fairness by design and default from the outset and the continuing prevalence of problematic practices. A further benefit is that consumer law has enhanced consumer trust in relation to digital transactions, evidenced by the significant longitudinal increase in the past 5-10 years in e-commerce and other digital markets. This is a benefit for traders as without consumer trust, the development of digital markets and services would be sub-optimal. It is difficult to attribute improvements solely to EU consumer law, as other factors such as increased digitalisation in the economy and society also play a role. Nonetheless, EU rules have provided the **necessary regulatory certainty and helped to foster more intra-EU trade**.

Regarding **consumer detriment**, the average EU consumer experiences problems several times a year, sometimes relating to legal gaps in the EU consumer law framework and on other occasions, due to poor compliance and a lack of effective enforcement of their rights. On average, one-third of consumers in the survey perceived that the problems encountered had caused them consumer detriment (either financial or non-financial harm, including harms such as time wasted due to inconvenience, e.g. not being able to cancel a contract, not being able to reach a person via a standard rate phone line). **Consumer detriment in the digital environment has been estimated at between EUR 6.1 bn and EUR 10.7 bn**. It is difficult to establish causality between consumer detriment experienced and legal gaps in the current regulatory framework as some detriment is caused by non-compliance by traders, whereas other detriment relates to lack of consumer education and awareness as to how to complain and seek redress. In addition, some practices are perceived as problematic by consumers but are not currently illegal.

In 2022, the European B2C e-commerce turnover increased from €849 billion in 2021 to €899 billion in 2022, despite a shifting economic and political environment. Although the growth rate for 2022, reaching 6%, compares lower than in 2021 (12%), the sector continues to move forward and is expected to continue growing in 2023. The consumer detriment estimated

would represent between 0.68% and 1.19% of the total value of e-commerce to consumers. This suggests that despite the seriousness of the problems encountered, a high volume of trading occurs without any problems being reported.

4.1.3 Relevance

The study demonstrated the **ongoing relevance of the general objectives of EU consumer law in meeting the identified needs of traders and consumers**, namely achieving high levels of consumer protection in the digital environment, and realising single market goals in a Digital Single Market context. The EU consumer law framework is relevant for the identified needs both offline and in the digital environment over the 30-year timeframe since the legislation first emerged (e.g. UCTD, since 1993, UCPD since 2005 and the CRD since 2011). The challenges for consumers addressed through EU consumer law remain highly relevant. These relate to the prevention of unfair, misleading, or aggressive practices and unfair contract terms, and ensuring sufficient information provision at pre-contractual and contractual stages. The general principles-based approach (UCPD, UCTD) has generally ensured that the legal framework has sufficient flexibility and maintained ongoing fitness for purpose over a prolonged period.

However, **over-reliance on the general principles-based approach raises issues about the relevance of the consumer law framework looking ahead, without more specific rules in at least some areas** to provide the regulatory certainty needed. Major EU legislative developments have taken place in digital and data laws and there has continued to be rapid evolution in digital markets, services and the types of traders active in the DSM. More specific rules could provide greater regulatory certainty and increase traders' familiarity with consumer law applicable in specific areas (e.g. persistence of dark patterns, online subscription traps).

In this context, there were **divergent views among stakeholders regarding whether further legislative changes are necessary**. Traders and their associations typically viewed the general principles-based clauses as being future-proofed, if supported by sufficiently frequent updates of the Commission's guidance. Consumer associations and some Ministries and CPAs agreed that the general principles-based approach should remain a central feature of the legal framework in ensuring wide coverage of problematic practices (including those that could emerge in future that could not have been foreseen). However, such stakeholders also perceived that there are problematic practices where regulatory action may be needed, such as the protection of minors online and tackling digital addiction.

The relevance of EU consumer law was found to be **undermined by the presence of digital asymmetries (structural, technological, informational)**, which go beyond the traditional informational asymmetries and power imbalances between traders and consumers. The increased prevalence of AI and algorithmic decision-making make it disproportionately difficult for consumers to understand the commercial practices they face and to verify whether their rights are being respected. Digital tools such as virtual assistants and price comparison websites can be used to overcome some informational asymmetries. However, some stakeholders favoured regulatory action to address these growing imbalances, through a possible alleviation of the burden of proof by allowing wider use of rebuttable presumptions at least in some circumstances where technologies are opaque from the perspective of the average consumer.

Future-proofing the EU consumer law framework will require further **stakeholder engagement to build consensus regarding the optimal regulatory architecture**, especially the balance between general consumer protection provisions and more specific rules. A clear trend can be noted towards more specific rules to regulate certain problematic practices in the digital environment both within some EU Member States and in third countries. However, there are also potential disadvantages as regulating specific business practices could become a challenging endeavour, given how quickly these evolve. New rules could

themselves quickly become outdated, in contrast to the general provisions, which allow application of the general fairness test on a case-by-case basis and interpretation by courts to provide regulatory clarity.

In addition, it will be important to consider the **role of non-regulatory measures in strengthening the effectiveness of the existing legal regime**. Should more specific EU consumer protection rules also be introduced in certain areas in future, awareness-raising about these will be needed to ensure that consumers are able to exercise their rights. These could include updating the Commission's Directive-specific guidance, efforts to raise awareness among consumers about their rights through consumer education and awareness campaigns, and CPAs proactively communicating with traders to raise awareness about their obligations. The latter would help to strengthen compliance. In parallel with possible regulatory and non-regulatory measures at EU and national levels, traders should be encouraged to play a positive role, e.g. through codes of conduct and the wider identification and sharing of good practices.

4.1.4 Coherence

There is **strong coherence between the UCPD, UCTD and CRD**, which each have their respective specificities but are mutually complementary and share common general objectives. The study did not detect many problems of internal coherence, apart from a few technical issues.

As regards **external coherence with other types of EU law**, the relationship is characterised by the application of other laws 'without prejudice' to EU consumer law. Other legislation can be implemented in parallel with consumer law, which remains applicable as a safety net, except in cases where the specific rules prevail. However, there is nonetheless an ongoing challenge in ensuring full coherence between EU consumer law and other legislation, both in terms of interpretation and diverging enforcement structures.

The rapid development of other EU laws in the digital area, such as the DSA, DMA, DCD, AVMSD, AI Act, GDPR, e-PD, make for considerable complexity, with traders, courts and enforcement authorities being required to apply consumer law in parallel with other legislation. There are **perceptions of outstanding legal gaps, inconsistencies and/or a lack of sufficient regulatory clarity on how consumer protection has been ensured in the digital environment across emerging digital markets and services**. For instance, the introduction of more specific rules in the DSA on the use of sensitive data for personalised advertising and the targeting of minors exacerbates the absence of such consumer rights in consumer law and leads to possible incoherence in jurisprudence and enforcement. Furthermore, greater alignment is necessary between the UCPD and the DSA in regulating dark patterns, between the UCPD, DSA and the GDPR in respect of personalised advertising, and between the UCPD and the AVMSD in respect of influencer marketing. Furthermore, the application of EU consumer law largely relies on courts and CPAs taking enforcement actions ex-post, either by following up on complaints or by initiating an own-initiative investigation, which can be contrasted with the ex-ante regulatory focus on technical standards in legislation such as the DSA, DMA and AIA.

The study also identified a **global trend towards countries prominent in digital markets and services introducing more specific rules in the digital environment to achieve consumer protection** (e.g. France, Germany, the Netherlands, Spain, and outside the EU-27, the US and the UK). The development of such national rules – and the scope for their future proliferation – presents a clear risk that the coherence and relevance of EU consumer law will be undermined in the absence of further EU action.

4.1.5 EU added value

Generally, most stakeholders perceived there to be **high EU added value from EU consumer law and its applicability in the digital environment** in delivering a balance between facilitating trade within the Digital Single Market (DSM) and ensuring high levels of consumer protection. Consumer representatives and traders alike acknowledged the important and beneficial role that EU consumer law plays. **Consumers emphasised the additional confidence that harmonised consumer rules bring in enabling them to make transactions online**, including cross-border, knowing that they will have certain rights irrespective of where they shop or sign up to online content or services, whether paid or free. Traders stressed the benefits of consumer law in facilitating the development of cross-border trade within the DSM. However, concerns were raised regarding the recent trend towards some MS introducing additional national rules, which risks undermining the benefits of harmonisation and the potential imposition of the costs of complying with national rules in addition to those arising from EU consumer law.

In a counterfactual situation in which there was an absence of EU consumer law, there would have been **lower levels of consumer protection in the digital environment due to a patchwork of 27 different sets of national consumer law** that would have otherwise existed to prevent unfair practices or contract terms. There would also have been no DSM benefits for traders if EU consumer law as applied in the digital environment across the EU-27 did not exist. This was estimated to have had a significant impact, given the increased size of the European digital economy, which has grown markedly in the past decade.

To ensure continuing EU added value, there is a need to **strengthen the clarity of the inter-relationship between consumer law and other new digital laws** to ensure adequate regulatory alignment and regulatory certainty for traders and consumers.

4.2 Recommendations

Recommendations of a strategic, rather than a technical, nature are presented in this section. Given that the study scope covered many different problematic practices, detailed ideas on possible technical solutions to address these practices are identified under the relevance criterion and in case studies, where a series of research questions are answered regarding possible ways forward in addressing problems with maintaining ongoing fitness for purpose.

4.2.1 Regulatory measures

Recommendation 1: The Commission should review the assessment of legal gaps in this study under relevance and external coherence to consider strengthening the legal framework and updating EU consumer law where appropriate to reflect developments in data and digital laws. The legal gaps analysis and review of external coherence with other relevant EU laws showed several areas where the interactions within the legal framework need to be reviewed by EU regulators. Examples include: the UCPD has not been modernised to reflect the growing role of data in the European data economy, even if the GDPR and DSA provide protection when applied in conjunction with the UCPD.

Recommendation 2: Digital fairness could be strengthened if the problem of digital vulnerability due to digital asymmetries was explicitly addressed in the provisions of EU consumer law and acknowledged in the recitals. Whereas the conceptual distinction between the average consumer and a vulnerable consumer in the UCPD has worked well for many years, the development of digital asymmetries has led to further structural, architectural and informational asymmetries. The concept of the digital vulnerability for consumers, including situational vulnerabilities, needs to be recognised as being different from the existing

definition of a vulnerable consumer.

Recommendation 3: Unfair, misleading and/ or aggressive dark patterns should be explicitly regulated in the UCPD, ideally through a 'digital fairness by design' provision.

This would ensure that traders reflect upon digital fairness in the design and development of online choice architectures, thereby eliminating many problematic practices analysed in the study. Dark patterns have a strong horizontal dimension. Fairness by design has the potential to enhance consumer protection from the outset of the design process, thereby strengthening consumer protection during all stages of transactional decision processes made by consumers.

Recommendation 4: EU consumer law should be updated to incorporate a number of key definitions relevant to achieving digital fairness. Some suggestions involve updating current definitions, whereas others relate to new definitions needed to ensure high levels of consumer protection in the digital age. For example, the notion of the '**average consumer**' should reference the real behaviour of consumers and the additional vulnerabilities consumers face in the digital environment due to digital asymmetries. The notion of '**consumer vulnerability**' should also be updated. Age should be more clearly defined, while children and minors should be afforded further specific protection, especially regarding data-driven personalisation practices and preventing the profiling of minors. There is also a need for better defining **coercion and harassment** by ensuring the definition includes a digital and not only a physical dimension.

Recommendation 5: The importance of data-driven personalisation practices should be reflected in the UCPD, which does not address data at all, despite its fundamental importance to the business models of many traders across digital markets and services, but also from a consumer perspective in the digital environment. Given the importance of data to the European digital economy, the absence of references to data makes the UCPD look outdated. For example, as children are especially vulnerable, using data profiling to personalise targeted ads should be banned for all traders, not only online platforms. Likewise, the use of sensitive data for targeted ads should be prohibited for all traders. Furthermore, the **inter-relationship between the UCPD, UCTD and the GDPR in the context of data used for personalisation practices should be clarified.** Whilst this is already mentioned in the guidance, more could be done by including a clear explanation in the recitals, and by including relevant definitions of personal and non-personal data. **Given privacy considerations, EU consumer law should provide consumers with real choices as regards data-driven personalisation.** Whilst recognising consumers may often benefit from personalisation, consumers need genuine choices regarding how far they consent to the sharing of data used for personalised commercial practices. Consumers need to be put in control of their data.

Recommendation 6: The Commission should debate with national Ministries and other stakeholders as to whether separate rules for influencers are needed. Whereas some MS have already regulated influencers (e.g. FR), there is a question of how far this is necessary, as the problem appears to stem primarily from a lack of awareness and understanding about existing requirements. **A typology of influencer activities is necessary to clarify which practices or actions qualify an influencer as a trader, and which do not.** The legal obligations and responsibilities of all relevant actors involved are unclear.

Recommendation 7: More specific rules should be introduced in certain areas of problematic practices related to digital contracts. Subscription traps should be prohibited by ensuring that it is as easy to exit as to enter into a subscription, subject to respecting a cancellation timeframe. It is unacceptable if traders make it overly cumbersome to cancel contracts during the cancellation period. **A cancellation button/function should be introduced, but with flexibility for traders as to how to comply.** The principle outlined

in the UCPD Guidance that “it should be as easy to exit from a subscription as to enter into it” should be codified, including to mirror the DSA and forthcoming changes to the CRD (through DMFSD amendments) regarding the 14-day withdrawal button. A contract cancellation button should be considered at EU level, with flexibility as to how to comply. This would aim to encourage innovation in improving the user-friendliness of interfaces, as an overly-prescriptive approach would go against technology-neutrality. Whilst the cancellation button is a possibility for websites, the technical means via which traders ensure that consumers can cancel a contract within the cancellation period should not be prescribed to ensure technology-neutrality. Alternatives, such as cancelling by email and/ or exercising cancellation rights via device and app settings should be allowed. Any alternative means used must be as straightforward as a cancellation button. Moreover, **advanced reminders that a free trial is about to convert into a paid subscription (e.g. to ensure active rather than passive consent) and reminders ahead of a subscription renewal are necessary.**

Recommendation 8: Transparency should be further improved but only in limited areas, to avoid consumer information overload. For example, transparency could be further enhanced in the area of **B2C personalisation, such as the personalisation of prices.** Whilst the CRD now contains (due to the MD amendments) a consumer right to be informed that a price has been personalised, this does not require an indication of the general criteria used in price personalisation or whether this is beneficial or disadvantageous to the consumer. Furthermore, there should be full transparency from traders about the actual price of **virtual items in video games in FIAT currency**, which should be provided in addition to any prices being displayed in intermediate currencies.

Recommendation 9: The UCPD’s Annex I of blacklisted practices has proven to be a valuable tool for prohibiting practices that cause consumer detriment. Several practices could be added to the Annex I to update and modernise it. Updating the blacklist would provide regulatory certainty more quickly than waiting for emerging case law. The practices prohibited in the blacklist are too specific to be included within the provisions and its updating could avoid overly-detailed practices being added into the core legislation. A risk of including such practices in the core provisions is that as soon as some practices are included, others would emerge, and therefore the legislation would become quickly outdated. In contrast, the Annex could be reviewed periodically, to ensure fitness for purpose. Examples of unfair practices that could be blacklisted in the UCPD include **various dark patterns** such as hidden charges, “sneak into basket”, confirm-shaming, aggressive practices that make it difficult for consumers to exercise cancellation rights, unnecessarily complicated and time-consuming interfaces to opt out of personal data sharing.

Recommendation 10: A blacklist of standard contract terms in the UCTD should be harmonised to strengthen digital fairness and to improve the efficacy of EU consumer law in the Digital Single Market. In the digital age, the absence of a common list of prohibited standard contract terms at EU level is notable, especially given the increasing globalisation and pan-European nature of many contract terms, as well as the global nature of digital markets and services. This could work in parallel with the more specific list of outlawed standard contract terms at national level. This would not prevent MS from continuing to maintain their own lists of prohibited contract terms, which could continue to run alongside an EU-wide mapping of such terms. Over the longer-term, this would help to harmonise prohibited contract terms whilst at the same time recognising the reality that national contract laws and business practices vary across the EU-27.

Recommendation 11: There should be a reversal of the burden of proof in specific circumstances by using rebuttable presumptions, such as if the technologies concerned are opaque, given the likely knowledge of the average consumer. This would recognise digital asymmetries that are more pronounced due to the use of AI systems and algorithms, and the average consumer cannot easily enforce their rights.

Recommendation 12: Strengthen the protection and rights of minors within EU consumer law generally. This would help to bring consumer law into closer alignment with other areas of EU law where children and minors have more specific protections. In particular **coherence between the DSA and the UCPD should be strengthened in respect of minors' rights by ensuring that the prohibition on the use of minors' personal data for personalised targeted advertising purposes** is extended to all traders (beyond those currently falling within the DSA's scope, such as platforms and marketplaces). This could ensure uniform protection for children irrespective of the type of trader and medium through which transactions are made. Furthermore, **principles relating to age-appropriate design could be considered at EU level to complement the suggested introduction of digital fairness by design and default provisions.** A preventative approach focusing on avoiding harm to children in unfair commercial practices by design should be embedded from the outset. This would also help to tackle the problem of digital addiction. In the area of video games, **uncertainty-based reward features such as loot boxes should be subject to stricter regulation.** There should be transparency about randomisation odds, and tools should be provided by developers, especially parental controls to easily disable their use or set spending limits.

4.2.2 Strengthening enforcement and monitoring

Recommendation 13: Enforcement should be further strengthened and reinforced both at EU and national levels, drawing on the existing regulatory powers under the CPC Regulation. Encourage CPAs to take on strategic deterrent cases to test the legal ground in respect of the application of EU consumer law in the digital environment, especially where rules contained in several pieces of law are concerned, such as between the UCPD, UCTD and the GDPR. This would establish precedents in the relative absence of case law in the digital environment and could have an outsized impact on trader compliance levels and/ or behaviours.

Recommendation 14: The **CPC network** should continue to play an important role in the implementation of consumer rights using the tools at its disposal, such as issuing recommendations, conducting website sweeps, and advising the Commission on the evolution in new and emerging unfair practices, etc. The CPC Network could also potentially play a stronger role in collecting complaints data disaggregated by business area, with a clearer distinction in the data collected by national CPAs necessary such as to be able to identify cases relating to the digital environment and to digital fairness. **There should be more even enforcement in the digital environment across the EU by CPAs, including through Joint Enforcement Actions by the CPC Network.** Only a few national CPAs have been proactive in taking on deterrent cases in the digital sphere. This has resulted in relatively few legal cases overall and led to time lags in case law emerging that could help to provide regulatory certainty, in a situation where there is increased complexity in applying consumer law with digital and data laws.

Recommendation 15: CPAs should invest in strengthening their technical and human resource capacity to undertake enforcement activities in the digital environment. Some have set up their own dedicated units to deal with cases in the digital sphere to improve assessment of digital fairness, but more should take similar steps. **Consider the greater use of automated tools and standard checklists to facilitate compliance checks by CPAs of traders with EU consumer law obligations in the digital environment.** For instance, web crawlers could automatically check some aspects of compliance (e.g. obligation to pay button, right of withdrawal button, ease of cancellation), and other digital tools could also be used to improve efficiencies e.g. automated detection of fake reviews, price hikes due to scalping bots.

Recommendation 16: National authorities responsible for consumer protection, data

protection, competition law and digital services legislation should work much more closely together, given the inter-relationship between these areas of law, which sometimes raises complex regulatory, compliance and enforcement issues. The Commission, the European Data Protection Board and the CPC Network could play a positive role in making this happen in practice.

Recommendation 17: A public database could be developed mapping the types of dark patterns used and providing anonymised illustrations of non-compliant practices. The worst of these practices could be added to the blacklist.

Recommendation 18: Monitoring through consumer surveys should be carried out periodically (e.g. every three years) to ascertain whether progress towards digital fairness has been made. Longitudinal tracking of problematic practices and how these have evolved over time is necessary to inform policy-making in future. This would facilitate establishment of clearer baselines and enable data-driven assessment of the scale of the problem and level of consumer detriment on a more consistent and comparable basis. Digital markets and services continue to grow, therefore the problematic practices analysed in this study should continue to be tracked.

4.2.3 Non-regulatory measures

Recommendation 19: Additional guidance is necessary for traders on how to comply with consumer law, including how to avoid common pitfalls in website and interface design leading to dark patterns. Dark patterns are complex, given there are many different types and there is a need to strengthen awareness among traders about how to improve practices through digital fairness by design and default.

Recommendation 20: Targeted consumer awareness-raising and education campaigns are needed about EU consumer protection rules in the digital environment. Consumers need to be better informed regarding how to ensure their rights are respected. For instance, many consumers experiencing perceived unfair problematic practices either did not complain in the first place, or if they made an initial complaint, did not take action to enforce their rights.

Recommendation 21: Improved cooperation is needed between regulators, consumer and trader representatives to address power imbalances/ digital asymmetries by empowering consumers and by bringing stakeholders together in a way that fosters innovative approaches to tackling problematic practices, such as an increased role of codes of conduct, standards, etc. In this context, **joint codes of conduct could be developed in thematic areas where problematic practices have been identified.** Voluntary initiatives by traders and their representative associations should be encouraged, including to ensure that consumer-friendly and compliant business practices are replicated more widely by all traders. In this regard, good practices could be shared for instance through development of business-friendly good practices ensuring digital fairness, in a way understandable for SMEs too. This would be complementary to the consumer law guidance documents on each Directive, which whilst providing very helpful examples, are more legalistic. More could be done to foster standards of fair design in online design interfaces and choice architectures. Standards could be promoted through the use of quality-labels that over time consumers would come to recognise, thereby promoting trader transparency and enhancing consumer trust. Approaches to develop fairness by design approaches could include the use of regulatory sandboxes in which regulators work together with major e-commerce providers and platforms on the development of standards for consumer interfaces, with inputs from consumer organisations to ensure that the process considers the everyday experiences of consumers in the digital environment.

4.2.4 Importance of a holistic approach to strengthening consumer protection in a digital fairness context

Recommendation 22: The Commission should take a holistic approach to strengthening the effectiveness of EU consumer law, ensuring its ongoing relevance and maximising its added value. Whilst this study has identified examples of non-compliance by traders and of problematic practices in emerging areas of digital markets and services, additional regulation alone will not address the complex series of issues identified. This implies a combination of: (1) regulatory measures to improve legal clarity; (2) non-regulatory measures, such as regular updating of guidance to include examples specific to different sectors across digital markets and services; (3) awareness-raising and consumer education about how to achieve redress when consumers suffer detriment, and training for groups of traders (e.g. influencers) where compliance levels are low; (4) more proactive enforcement from a wider range of national CPAs to improve the strategic deterrent effect of enforcement activities and an enhanced role for case law (recognising the paucity of legal cases pertaining to EU consumer law's application in the digital environment), which could strengthen regulatory certainty in a more timely manner; and (5) close regulator-trader cooperation.

