The Digital Fairness Act

Getting ready for the next wave of EU consumer regulation

For what comes next

tlt.com

Introduction

You may have heard about the EU Digital Fairness Act (DFA), but what is it? And what will it mean for digital platforms in the EU?

The first thing to note is that while the term 'DFA' is widely used, for now it is no more than a proposal. There is no draft legislative text.

However, the European Commission (the Commission) is expected to bring forward legislative proposals later this year (2026) aimed at strengthening consumer protection in the digital environment.

This builds on the findings of the **Digital Fairness Fitness Check**, which concluded that existing consumer rules are not sufficiently adapted to address the complex and evolving practices consumers face online.

While the legislative scope of the DFA remains undecided (and hotly contested), it is expected to focus on a range of digital practices.

This guide is designed to help you understand what the DFA may have in store, but it's important to remember that nothing is set in stone yet. We cover seven key digital fairness policy issues, looking at how existing EU law applies, what the DFA could change, and key points to be aware of now.

We hope you find this guide useful in planning for the year ahead. If you have any questions about these changes or would like assistance in preparing for them, please **get in touch**.

Click on the icons to navigate to each section of the report.

Legislative and policy context

1. 'Dark patterns' and deceptive design practices

2. Engagement driven design features

3. Video games and interactive entertainment

4. Unfair personalisation practices

5. Social media influencers

6. Unfair pricing practices

7. Subscriptions and digital contracts

Legislative and policy context

In May 2022, the Commission launched the Digital Fairness Fitness Check to assess whether the Unfair Commercial Practices Directive (UCPD), the Consumer Rights Directive (CRD), and the Unfair Contract Terms Directive (UCTD) remained fit for purpose. The conclusions, published in October 2024, found gaps and legal uncertainty in the current principle-based framework, particularly in relation to system design and complex digital commercial practices.

This was followed by a public consultation and call for evidence between July and October 2025. Despite opposition from a number of industry stakeholders, who argued that the EU's digital regulatory landscape is already highly complex, overlapping and inconsistently enforced, the Commission's **2030 Consumer Agenda** confirmed its intention to propose a DFA in late 2026.

The precise legislative form remains open. The proposal may take the form of a standalone regulation, targeted amendments to existing directives, or a combination of both.

One option thought to be under consideration is converting the existing UCPD framework from a Directive to Regulation with direct effect across all EU member states. This would have the effect of putting EU consumer law on the same legislative footing as GDPR.

In terms of enforcement, the Commission is also running a parallel workstream to review the CPC Regulation, which may result in tougher, more harmonised enforcement of EU consumer law.

What are the timescales?

The Commission has not committed to a firm legislative timeline for adopting the DFA. However, it has indicated that it intends to bring forward a proposal later in 2026, with the DFA included in the 2026 Commission Work Programme as a Q4 2026 initiative.

The full legislative timetable will then be informed by whether the Commission seeks to introduce a new regulation – as it did with the Digital Services Act and Digital Markets Act – or whether it will seek to introduce a new Omnibus Directive updating the existing framework of consumer protection directive (or potentially a combination of both).

Either way a reasonable expectation for adoption – assuming the proposals make it that far – would be somewhere between 2028 – 2030. Again, this will depend on whether the proposals take the form of a regulation with direct effect or directives, with the latter requiring longer for national implementation at Member State level.

However, it is important to emphasise that the EU legislative process offers no guarantees. Wider geopolitical factors could prompt a change of course in the future, particularly when it comes to adding further regulatory costs for trading in the EU at a time when Europe's global competitiveness is under the spotlight.

Key digital fairness policy issues

Issue 1: Dark patterns and deceptive design practices

The Commission's Fitness Check found that so-called 'dark patterns' undermine consumers' ability to make free and informed decisions and are widespread across digital services, with one study identifying them on 97% of popular websites and apps[1].

There have increasingly been calls to move away from the nefarious term 'dark patterns', but this broadly refers to deceptive design practices and harmful forms of online choice architecture.

Design techniques repeatedly highlighted by the Commission include click fatigue, confirm-shaming, misleading urgency or scarcity cues, nagging prompts, sneaking items into baskets, ambiguous or double-negative language, and presenting choices in a leading or non-neutral manner.

How existing EU law applies

- Deceptive digital design practices could be deemed an 'unfair commercial practice' under the UCPD if it is likely to deceive the average consumer into taking a transactional decision they would not otherwise have taken. Some practices (e.g. 'nagging' via push prompts) have the potential to be regulated as aggressive commercial practices. In practice, the evidential threshold for regulators is high, and whilst the UCPD contains a blacklist of practices prohibited in all circumstances, none relate specifically to digital interface design.
- Dark patterns are also regulated under Article 25 of the Digital Services Act (DSA), which prohibits organising or operating online interfaces in a way that deceives or manipulates users in a manner that materially distorts or impairs their ability to make free and informed decisions. However, this provision does not apply where the UCPD or General Data Protection Regulation (GDPR) already regulate the practice, which has prompted confusion as to the practical scope of Art.25 of the DSA in B2C scenarios. This is a good example of how overlapping regulation of deceptive design practices is already creating uncertainty.
- From an AI regulation perspective, Article 5(1)(a) of the EU AI Act prohibits AI systems that deploy subliminal, manipulative or deceptive techniques to materially distort a person's behaviour by impairing their ability to make an informed decision and causing them to take a decision that they would not otherwise have taken in a manner that causes significant harm.

Consumer protection law does not exist in a vacuum and deceptive design techniques also trigger other adjacent regulatory regimes. For example, GDPR Articles 4(11) (definition of consent) and 7 (conditions for consent) require consent to be freely given, specific, informed and unambiguous. Dark patterns that steer consumers towards consenting to data processing may invalidate that consent.

From a competition perspective, large tech companies that are designated as 'gatekeepers' of core platform services under the Digital Markets Act (DMA) are also subject to stringent rules governing choice architecture to ensure fair and open competition – for example default browser choice.

What the DFA could change

The DFA is intended to address the consumer protection gaps identified by the Commission. Potential measures include:

- **Expanded blacklist**
  Specific design features may be added to UCPD Annex I, creating automatic prohibitions without the requirement to prove that the practice successfully influenced the consumer's behaviour.
- **Fairness by design**
  The DFA may introduce a fairness by design duty, requiring traders to proactively ensure their interfaces protect consumer autonomy from the outset. A proposed "grey list" would create a rebuttable presumption of unfairness for certain commercial practices, effectively shifting the burden onto businesses to justify questioned design.
- **Harmonised definitions**
  New EU-wide definitions for specific dark patterns are expected to replace current legal ambiguities and support consistent enforcement.
- **Reversal of the burden of proof**
  In technology complex cases, the DFA may require businesses to demonstrate that their digital commercial practices comply with consumer protection law. This would apply where consumers, interested parties or authorities face disproportionate difficulty in accessing the information needed to evidence a trader's wrongdoing, materially shifting evidential risk onto businesses.

Key takeaways

Regulatory scrutiny of user journeys and interface design is intensifying, with regulators increasingly expecting businesses to demonstrate that design choices do not undermine consumer autonomy.

In practice, this will likely require much closer coordination between legal, UX, product and data teams, alongside stronger governance and clearer documentation of personalisation, experimentation and A/B testing decisions.

Businesses that proactively review higher-risk design patterns (such as subscription flows, consent prompts and targeted personalisation) will be better placed to anticipate regulatory direction as the DFA regime takes shape, rather than reacting once enforcement expectations crystallise.

Issue 2: Engagement-driven design features

Engagement-driven design features, including infinite scroll, autoplay, streaks, variable reward mechanisms and algorithmic feeds, have become increasingly common across digital services.

This has led to an increase in regulatory scrutiny from consumer activist groups who contend that some of these features may be addictive and should be regulated. Whether it is appropriate to characterise these kinds of features as addictive is a highly sensitive and complex area, not least because it strays into cognitive science and psychology. UX designers are tasked with designing interfaces that make their app or website satisfying for users. When does this 'tip' into behaviour that should be classified as unlawful under consumer law?

Nevertheless, the Commission has concerns that engagement-driven features can lead users to spend more time or money online than intended. Its Fitness Check concluded that existing EU consumer protection rules, while still relevant, do not fully address issues raised by design-driven engagement techniques, particularly regarding children and adolescents.

How existing EU law applies

There are few prescriptive, targeted consumer protection laws governing this area in the EU.

Most of the enforcement to date has been carried out by the Commission under the DSA against designated very large online platforms (VLOPs) with over 45 million monthly active users in the EU. Articles 34 and 35 require the assessment and mitigation of systemic risks, which the Commission has confirmed include risks to users' physical and mental wellbeing arising from platform design and recommender systems. Article 28 introduces specific protections for minors, and Commission guidance recommends disabling high-engagement features such as autoplay, streaks and certain notifications by default for children.

While social media providers have been scrutinised for the way their platforms are designed, the Commission has also considered the deployment of engagement-driven features in e-commerce by online marketplaces that are designated as VLOPs.

For example:

- In October 2024, it **opened formal proceedings against Temu**, investigating risks linked to the allegedly addictive design of the service, including game-like reward programmes designed to incentivise repeat purchasing and the adequacy of Temu's systems to mitigate risks to users' physical and mental wellbeing.
- In February 2026, a **similar investigation was launched into Shein**, focusing (amongst other things) on engagement-driven features such as giving consumers points or rewards and their potential negative impact on user wellbeing.

Both the Temu and Shein cases are notable for targeting e-commerce gamification mechanics, loyalty points, reward-based engagement loops and game-like incentive structures. The consumer harms associated with engagement-driven design features in social media tend to focus on broader wellbeing and societal concerns, particularly for younger users, whereas the e-commerce features under scrutiny in the Temu and Shein proceedings are more directly linked to protecting consumers' wallets, specifically the risk that gamification mechanics encourage users to spend more than they otherwise would.

For traders that are not designated as VLOPs under the DSA, the deployment of engagement-driven design features could be regulated as an unfair commercial practice for the purposes of the UCPD, particularly if they are deployed in a misleading way or aggressively influence transactional decisions. However, as noted above, it can be difficult to determine when engagement-driven features intended to enhance user experience tip into unlawful practice. As a result, enforcement of the UCPD at national level has (unsurprisingly) been limited.

What the DFA could change

Regulatory intervention here is difficult, not least due to overlapping theories of harm between digital wellbeing and economic consumer protection. Designing a clear, coherent framework that doesn't inadvertently prohibit legitimate UX practices remains a significant challenge for EU lawmakers. Some of the policy proposals that have been put forward include:

- **Age-specific feature restrictions**
  Engagement-driven features such as infinite scroll, autoplay, streaks and variable-reward notifications may be prohibited for minors or switched off by default, subject to controlled opt-in.
- **Mandatory usage controls**
  Websites and applications widely used by children and adolescents may be required to implement break reminders, session caps, inactivity prompts and clearer usage dashboards to counter excessive use.
- **Stronger age-assurance expectations**
  Proposals for a harmonised minimum age of 16 for access to certain social media services and AI companions remain under discussion, potentially alongside stricter age-assurance obligations.

Key takeaways

The trajectory points towards design-level accountability, with businesses expected to demonstrate how engagement techniques align with consumer autonomy and wellbeing. Increased scrutiny of high-retention features is likely, particularly where minors are concerned.

Early mapping of engagement-driven design patterns, recommender logic and age-based user journeys will place organisations in a stronger position as the DFA regime takes shape.

Issue 3: Video games and interactive entertainment

The video games and interactive entertainment sector has evolved from one-time purchase models into complex monetisation ecosystems involving virtual currencies, randomised rewards and engagement-driven mechanics.

Loot boxes, defined as randomised reward mechanisms purchased using real-world or virtual currency, are attracting increasing scrutiny, with critics arguing that they exploit psychological vulnerabilities in ways comparable to gambling, particularly among younger players.

Regulation across Europe remains fragmented, and the forthcoming DFA could introduce a more harmonised EU-wide framework addressing loot boxes, virtual currencies and pay-to-progress mechanics.

It's important to note that these issues aren't limited solely to the gaming industry. For example, 'gamification', (including digital items and virtual currencies) is now prevalent across a number of areas, including e-commerce and social media.

How existing EU law applies

Game developers are already subject to a number of consumer protection regulations under EU law, albeit these are not specifically targeted at the gaming industry.

For example:

- Misleading claims about the odds of receiving particular items, or artificial scarcity signals, could in principle be caught by the UCPD's prohibitions on misleading and aggressive practices. However, the UCPD does not specifically require disclosure of loot box probabilities and does not directly regulate monetisation structures.
- Consumers have a 14-day cancellation right for distance contracts under the CRD, but this is routinely excluded for digital content once performance begins with consumer consent.
- Gambling regulation remains primarily a matter for individual Member States, creating a patchwork of approaches. Belgium, for example, treats some paid loot boxes as illegal gambling, while other jurisdictions have introduced limited restrictions or continue to investigate. Loot boxes therefore sit in an uncertain space between gambling and consumer protection law, with neither providing a consistent EU-wide answer. Although the DSA and EU AI Act restrict certain manipulative or deceptive design, they are not designed to target video game monetisation mechanics.

What the DFA could change

Some measures that have been proposed include:

- **Greater transparency around in-game rewards and pricing**
  Mandatory disclosure of the probability of obtaining specific items from randomised reward mechanics, alongside requirements to display the real-world monetary value of in-game purchases, including where pricing is denominated in virtual currency.
- **Enhanced protections for minors and parental controls**
  The DFA could also restrict or prohibit loot boxes and randomised rewards for minors or require parental consent as a precondition for such purchases.
- **Potential limits on engagement-driven design features**
  There is also an overlap in this area with engagement-related design controls to regulate addictive design features. Some consumer activist groups have called for restrictions on autoplay, mandatory natural stopping points, spending limits and other friction-based safeguards.

Key takeaways

Game monetisation design is increasingly being scrutinised as a consumer protection issue rather than a niche gambling concern.

Developers may wish to map monetisation risk across the full player journey, including virtual currencies, loot boxes, time-limited offers and engagement mechanics, and test assumptions around the legal classification of in-game currencies.

More generally, the use of 'gamified' design features in other sectors could come under increasing scrutiny, particularly if they involve virtual coins or loot box style mechanics.

> Loot boxes sit in an uncertain space between gambling and consumer protection law, with neither providing a consistent EU-wide answer.

Issue 4: Unfair personalisation practices

The Commission's Fitness Check also identified an increase in consumer concern around unfair personalisation practices.

Research indicates that around 70% of consumers are concerned about how their personal data is used, and 37% believe that companies exploit knowledge of individual vulnerabilities for commercial gain.[2]

The Commission has also highlighted unease about the opaque nature of data collection and profiling, with many consumers reporting difficulty understanding the impact of profiling on the advertisements, content and prices they are shown.

How existing EU law applies

Personalisation is already subject to a number of overlapping EU privacy and consumer protection laws. Enforcement challenges remain, where consent, transparency and fairness standards intersect across regimes, creating uncertainty for businesses implementing compliant personalisation strategies.

For example:

- The CRD requires online traders to inform consumers where pricing is personalised based on automated decision-making. More generally, unfair personalisation practices may be prohibited under UCPD if they fall short of standards of professional diligence, particularly where they involve exploiting known vulnerabilities to unduly influence consumers' transactional decisions. The UCPD also imposes transparency obligations around ranking and paid placement in search results.
- Unfair personalisation practices are also regulated under the DSA. This includes transparency around recommender systems and, for VLOPs, a requirement to offer at least one recommender system option that is not based on profiling.

  The DSA also prohibits targeted advertising based on profiling using special categories of personal data or directed at minors.

  The Commission's **ongoing investigation into Shein** under the DSA is exploring potential unfair personalisation practices. The case is investigating whether Shein failed to provide an easily accessible alternative recommender system that is not based on profiling, and whether the main parameters of its recommender system were sufficiently clear.
- From a GDPR perspective, fairness and transparency principles provide safeguards against manipulative or opaque personalisation. It also restricts decisions based solely on automated processing that produce legal or similarly significant effects, permitting them only in limited circumstances and subject to safeguards. Where personalisation relies on tracking technologies, the ePrivacy Directive requires informed consent before information is stored on, or accessed from, a user's device.

- The EU AI Act also places clear limits on certain forms of exploitative personalisation. For example, it prohibits AI systems that exploit vulnerabilities linked to factors such as age, disability, or specific social or economic circumstances, with the objective, or the effect, of materially distorting behaviour in a way that could result in significant harm.

What the DFA could change

While personalisation practices are already subject to extensive EU regulation, the following additional policy measures have been proposed by consumer activist groups or regulators:

- **Further profiling restrictions**
  Extending existing prohibitions on targeting minors or using special category personal data beyond online platforms to all traders – thereby raising the standard for businesses that aren't designated as VLOPs under the DSA.
- **Situational vulnerability protections**
  Introducing new rules to prohibit the exploitation of temporary situational vulnerabilities, such as grief, financial distress, or emotional exhaustion. This would mirror the wider definition of 'vulnerable consumers' introduced by the UK Digital Markets, Competition and Consumers (DMCC) Act.
- **Price personalisation restrictions**
  Building on existing disclosure obligations to restrict certain forms of personalised pricing and requiring meaningful information about the logic used to determine a personalised price at the point of sale.
- **Right to non-personalisation**
  Another proposal that has been floated is that all digital traders – not just designated VLOPs – should offer a clear and accessible option to only receive non-personalised advertising and pricing.

> European Commission research indicates that around 70% of consumers are concerned about how their personal data is used, and 37% believe that companies exploit knowledge of individual vulnerabilities for commercial gain.

Key takeaways

As consumer regulators intensify scrutiny of the use of AI-driven personalisation and dynamic UX design, this has become a particularly sensitive risk area.

The DFA is likely to raise expectations around the design and operation of digital services, especially for businesses that aren't currently designated as VLOPs under the DSA, with a sharper focus on impacts for vulnerable consumers and minors. In practice, this will require targeted, risk-based reviews of profiling, personalisation and dynamic pricing practices.

Effective compliance is also likely to depend on closer coordination between legal, product, marketing and data teams, embedding a "fairness by design" approach that mitigates discriminatory outcomes and avoids exploitative personalisation.

Issue 5: Social media influencers

The Commission's Fitness Check highlighted that influencers have gained considerable power in shaping public discourse, but their commercial activities are often opaque.

A 2024 compliance sweep of 576 influencers found that whilst nearly all posted commercial content, only 20% systematically disclosed its commercial nature[3]. The Commission also identified concerns about influencers promoting harmful content, with 44% of consumers reporting seeing influencers promoting scams or dangerous products[4].

How existing EU law applies

- The UCPD applies to misleading or hidden advertising where it is likely to cause consumers to take a transactional decision they would not otherwise have taken. The framework also includes practices that are prohibited in all circumstances, such as direct exhortations to children to purchase products and certain forms of misleading or paid-for consumer endorsements. Commission guidance further clarifies that influencers are likely to be considered as "traders" where they receive any form of consideration, whether monetary or in kind, meaning their promotional activity must comply with the UCPD.
- Under the DSA, online platforms are expected to ensure that advertisements are clearly identifiable, and to provide functionality that enables influencers and other content creators to declare when content constitutes a commercial communication to their audiences.
- Related rules under the Audiovisual Media Services Directive also address risks associated with covert or harmful advertising practices. The regime is intended to prevent hidden or surreptitious audiovisual advertising, placing restrictions on the promotion of certain regulated products. It also includes enhanced protections aimed at safeguarding minors.

"A 2024 compliance sweep of 576 influencers found that whilst nearly all posted commercial content, only 20% systematically disclosed its commercial nature.

What the DFA could change

- **Harmonised EU definitions and disclosures**
  The DFA could introduce a clear, EU-wide legal definition of "influencer marketing" and "influencer". In addition, the consumer group BEUC have called for uniform, mandatory disclosures to make it easier for consumers to distinguish between organic content and marketing communications.

  This proposal is contentious because most large social media platforms already provide easily accessible tools that enable content creators to disclose commercial content.

- **Extended brand and agency liability**
  It has also been proposed that the DFA clarify and extend the circumstances in which brands and agencies are responsible for ensuring influencer compliance.

  While liability can already arise under the UCPD where misleading commercial communications are made on a brand's behalf, it has been suggested that the concept of joint liability should be made more explicit.

- **'Kidfluencing' protection**
  Measures aimed at protecting minors from commercial exploitation are likely to be a key focus, including potential restrictions on financial incentives for child content creators. This is one of the more concrete areas where legislative intervention has been openly discussed at EU level.

- **Restrictions on product claims**
  The DFA could extend and harmonise existing restrictions on the promotion of products such as unhealthy foods, dietary supplements, gambling services and unrealistic beauty standards across all content formats and platforms.

> The DFA is expected to introduce a more demanding and standardised compliance framework for influencer marketing, with increased scrutiny of disclosure practices and brand oversight.

Key takeaways

The DFA is expected to introduce a more demanding and standardised compliance framework for influencer marketing, with increased scrutiny of disclosure practices and brand oversight.

In practice, this will push businesses towards stronger contractual protections, more active monitoring and clearer governance, particularly for campaigns that involve minors.

Businesses in regulated sectors such as food and beverage, dietary supplements, gambling and beauty should also prepare for tighter restrictions across formats and reassess campaigns that rely on sector-specific regimes.

Issue 6: Unfair pricing practices

The Commission's Fitness Check highlighted drip pricing, misleading reference prices in dynamic pricing models, and inflated RRP comparisons as key areas of concern.

Whilst aspects of these practices are already addressed under existing EU consumer law, the DFA is expected to clarify and strengthen current rules. Consultation feedback showed strong support from consumer advocacy groups for introducing DMCC-style drip pricing rules and tightening controls on dynamic pricing, signalling that pricing transparency will be a central focus of the DFA.

How existing EU law applies

- The UCPD already prohibits misleading commercial practices relating to the price or the manner in which the price is calculated, or the existence of a specific price advantage.

  Certain pricing tactics are also prohibited in all circumstances, including bait-and-switch practices and false claims of limited-time availability or urgency. Commission guidance confirms that practices such as drip pricing, misleading price comparisons and certain forms of dynamic pricing may infringe these provisions, depending on context.
- The CRD requires traders to ensure that consumers are provided with clear and comprehensible information about the total price of a product or service, including mandatory taxes, service charges and delivery fees, before entering into a contract.
- Pricing transparency is also addressed under the Price Indication Directive. The regime is intended to ensure that selling and unit prices are presented in a clear, unambiguous and easily identifiable way. Following amendments made via the Omnibus Directive, any announcement of a price reduction must indicate the lowest price applied by the trader during a period of at least 30 days prior to the discount. This only applies to goods, not services.

> Consultation feedback showed strong support from consumer advocacy groups for introducing UK DMCC-style drip pricing rules in the EU.

What the DFA could change

The DFA is expected to seek greater consistency in pricing practices, moving away from purely case-by-case assessments towards more clearly defined standards. Potential measures include:

- **Outright prohibitation of drip pricing**
  The EU may follow the UK in clamping down on drip pricing. This could be via introducing amendments similar to those introduced in the UK DMCC Act, which force traders to comply with hardline price transparency requirements in all invitations to purchase. Or drip pricing could be added to the UCPD blacklist, which prohibits mandatory costs (such as processing or booking fees) from being added late in the purchasing journey.
- **Restrictions on dynamic pricing mechanics**
  Potential constraints on the use of "starting from" prices, including requirements that such prices be genuinely available to a meaningful number of consumers. The Commission is also expected to explore additional transparency obligations for real-time price changes, for example where prices fluctuate while consumers wait in virtual queues.
- **Tighter rules on reference prices**
  Further clarification of when a claimed price advantage (such as "30% off") may be advertised, including restrictions on comparisons based on artificial or inflated RRPs, to ensure reference prices reflect genuine market conditions.
- **Event ticket resale practices**
  Measures aimed at curbing artificial price inflation in secondary ticket markets, including potential restrictions on business-led resale of event tickets for profit where this distorts primary market pricing.

Key takeaways

The DFA is likely to bring closer scrutiny of pricing structures and discount claims, with an emphasis on consistency and transparency.

Given that unfair pricing practices are already tightly regulated under EU consumer law, businesses should review their pricing models now to ensure advertised prices, reference prices and fees are transparent, defensible and applied consistently across the customer journey.

Issue 7: Subscriptions and digital contracts

The rapid growth of the digital subscription economy has been accompanied by an increase in consumer complaints across the contract lifecycle.

The Commission's Fitness Check highlighted ongoing concerns including difficulties cancelling, automatic renewals, and free trials that convert into paid subscriptions without adequate consumer awareness or control.

How existing EU law applies

- The CRD provides consumers with a 14-day right of withdrawal for many distance contracts, including subscriptions, subject to established exceptions. For certain digital content and digital services, the withdrawal right may be lost where performance begins with the consumer's express consent and acknowledgement.

  Traders must also provide clear and comprehensible pre-contract information, including the contract duration, renewal arrangements, termination conditions and total price.

- This framework is being supplemented by Directive (EU) 2023/2673, which amends the CRD to introduce a requirement for a dedicated online withdrawal function for distance contracts concluded via an online interface, where a statutory withdrawal right applies. This obligation will apply from 19 June 2026, following Member State implementation.
- Making it unreasonably difficult for consumers to cancel a subscription could also constitute a misleading or aggressive commercial practice under the UCPD, particularly where dark patterns are used to deter or delay cancellation.

  Commission guidance highlights practices such as misleading free trials, confirm-shaming and unnecessarily convoluted cancellation journeys, and emphasises that cancellation flows should not be designed in a way that is materially more onerous than sign-up.

Several Member States have already gone further than the current EU baseline.

For example:

- Germany requires a prominently displayed online termination button for certain ongoing consumer contracts concluded online, and France has introduced online cancellation facilitation requirements and advance notice obligations linked to tacit renewal.

What the DFA could change

- **Simpler, equivalent cancellation mechanisms**
  Commission materials suggest the DFA may propose EU-wide rules requiring subscription contracts to be cancellable through equivalent means to those used for conclusion, potentially supported by standardised online functionality such as button-style mechanisms.
- **UK-style controls on subscriptions and renewals**
  One approach would be for the EU to adopt proposals that mirror the new subscription contract rules introduced by the UK in the DMCC Act (set to come into force in Spring 2027). This would involve stricter controls on automatic renewals, mandatory renewal reminders, and tighter controls around free-trial conversions, including offering an additional cooling-off period after a free-trial converts into a longer paid subscription.

Key takeaways

The regulatory direction points towards greater symmetry between sign-up and cancellation, tighter oversight of automatic renewals and free trials, and enhanced transparency throughout the subscription lifecycle.

Businesses developing new subscription products should factor these expectations in early when developing UX design, T&Cs and reminder notices for new subscription products to reduce the level of remediation required if the DFA introduces more stringent requirements as expected.

> If the EU adopts UK DMCC-style rules for subscriptions, this would involve stricter controls on automatic renewals, mandatory renewal reminders, and tighter controls around free-trial conversions, including offering an additional cooling-off period after a free-trial converts into a longer paid subscription.

Contact our digital consumer regulation team

Navigating the complex legal and regulatory frameworks that affect digital business is essential for those seeking to protect their innovation and maintain market leadership.

We provide strategic and operational support, helping our clients manage risk, unlock opportunity, and stay ahead of regulatory developments.

We regularly advise large digital platforms on complex consumer issues and complex investigations, including the recent changes to UK digital and consumer regime under the DMCC Act, providing technical compliance advice on fake reviews, pricing practices, subscription contracts, and online choice architecture.

Using our sector insight, we anticipate legal, regulatory, and commercial challenge, helping our clients navigate the digital landscape and creating opportunities for what comes next.

Richard Collie
Partner

richard.collie@tlt.com

Lorna Cropper
Partner

lorna.cropper@tlt.com

Lili Elenoglou
Legal Director

lili.elenoglou@tlt.com

Molly Efford
Senior Associate

molly.efford@tlt.com

Emily Rhodes
Senior Associate

emily.rhodes@tlt.com

Georgina Hands
Associate

georgina.hands@tlt.com

tlt.com

Belfast | Birmingham | Bristol | Edinburgh | Glasgow | London | Manchester | Piraeus

TLT LLP and TLT NI LLP (a separate practice in Northern Ireland) operate under the TLT brand and are together known as 'TLT'. Any reference in this communication or its attachments to 'TLT' is to be construed as a reference to the TLT entity based in the jurisdiction where the advice is being given. TLT LLP is a limited liability partnership registered in England & Wales number OC308658 whose registered office is at One Redcliff Street, Bristol, BS1 6TP. TLT LLP is authorised and regulated by the Solicitors Regulation Authority under ID 406297.

In Scotland TLT LLP is a multinational practice regulated by the Law Society of Scotland.

TLT (NI) LLP is a limited liability partnership registered in Northern Ireland under ref NC000856 whose registered office is at River House, 48-60 High Street, Belfast, BT1 2BE

TLT (NI) LLP is regulated by the Law Society of Northern Ireland under ref 9330.

TLT LLP is authorised and regulated by the Financial Conduct Authority under reference number FRN 780419. TLT (NI) LLP is authorised and regulated by the Financial Conduct Authority under reference number 807372. Details of our FCA permissions can be found on the Financial Services Register at https://register.fca.org.uk