Time to Riot!

How to respond to overbearing consumer protection

29 June 2026

The European gaming industry, like many digital sectors, is currently facing a perfect storm arising from an arguably incomprehensible – some might even say incoherent – patchwork of EU regulatory requirements. Driven by the European Commission's (*Commission*) ambition to establish digital sovereignty, the regulatory net has tightened, moving from general data protection (*GDPR*) to specific technical and behavioural obligations for companies. The following briefing breaks down the key legislation on consumer protection as well as its implications on the European gaming industry.

Key legislative pillars on consumer protection affecting gaming

- Digital Services Act (*DSA*): While initially perceived as a tool to regulate social networks, the DSA's functional definitions have brought the gaming industry directly into its scope; though its application depends on the classification as a 'service provider'. Generally, operators or publishers of multiplayer games (e.g. those hosting live-service environments) must comply with the DSA, while pure developers who do not provide the underlying hosting infrastructure fall outside the Act's primary obligations. This distinction follows from the application of the act to 'intermediary services', meaning games qualify as 'hosting services or online platforms' only if they store or disseminate user-generated content, ranging from simple chat logs and profile bios to complex player-created maps and skins. If applicable, the DSA mandates strict content moderation and prohibits so-called 'dark patterns' in interface design (particularly with regard to in-game stores). For these providers, rules on illegal content and transparency reporting are now standard operational requirements.

- Cyber Resilience Act (*CRA*): The CRA reclassifies games – whether distributed physically or more commonly via download – as 'products with digital elements', imposing horizontal cybersecurity requirements for the entire product lifecycle. This means that even digital-only software must now undergo conformity assessments and carry CE-marking (e.g. by documentation in technical files) to signal compliance with EU security standards. While full compliance is required by December 2027, the reporting obligations for exploited vulnerabilities become mandatory in September 2026. Developers must now notify the European Union Agency for Cybersecurity (ENISA) immediately after detecting an actively ex-

ploited vulnerability. Game developers must move from reactive patching to proactive security by design, ensuring that security support is guaranteed for at least five years, or face fines of up to EUR 15 million or 2.5% of their global turnover.

- **Artificial Intelligence Act (*AI Act*):** The AI Act's practical impact on gaming is significantly limited, as most sector specific AI applications (e.g. pathfinding, balancing, or NPC training) are, if at all, classified as minimal risk AI applications and remain unregulated. Currently, the AI Act only applies to the industry in narrow, exceptional cases. First, under transparency rules, studios using AI to generate hyper-realistic speech, faces, or events (so called 'deep fakes') must disclose this to the player. However, for the gaming industry, this obligation is notably light: because games should generally be recognised as fictional and artistic works, consequently developers are not required to provide intrusive, real-time warnings. Instead, a general disclosure – such as a notice in the end credits or a start-up splash screen – should be considered sufficient to meet the transparency standard. Beyond this, the AI Act establishes red lines for 'prohibited practices', strictly barring the use of AI for subliminal manipulation that exploits player vulnerabilities (e.g. exhaustion or age) to *inter alia* drive addictive spending or harmful engagement.

- **Data Act:** Focused on the internet of things, the Data Act requires that users have a right to access and share data generated by connected products and related services. Manufacturers of gaming hardware (VR, consoles) must ensure access by design by September 2026, allowing players to export raw usage data to third parties. For software-only developers, the Act's cloud-switching rules (already in force) significantly reduce vendor lock-in, providing the legal right to migrate backend infrastructures between cloud providers within 30 days without prohibitive exit fees.

- **Consumer Protection Cooperation Key Principles on In-game Virtual Currencies (*CPC Principles*):** Unlike a single legislative act, these principles represent a common enforcement position adopted by the Commission and national consumer authorities to address the lack of price transparency in 'dual-currency' ecosystems. They mandate that online games clearly disclose the real-world monetary equivalent of virtual goods at the point of purchase and prohibit deceptive 'free-to-play' labelling if the game contains unavoidable microtransactions. However, as these principles rely on the coordinated, yet often inconsistent, action of individual national competent authorities, they currently function more as a 'soft law' framework. For developers, this creates a fragmented compliance landscape where the risk of enforcement varies significantly across Member States, serving as a precursor to more rigid, codified consumer protection standards.

The proposal for the Digital Fairness Act is expected to land in 2026

Scheduled for a formal proposal in Q4 2026, the **Digital Fairness Act (*DFA*)** is set to become the final pillar of the EU's digital consumer framework. While the DSA governs platforms and content moderation, the DFA will cut deeper into the economic design of digital products. It specifically targets the intersection of behavioural psychology and monetisation, aiming to regulate how developers drive engagement and influence consumer spending.

The DFA stems from the 2024 *Digital Fairness Fitness Check*, which concluded that while current laws (Unfair Commercial Practices Directive or Consumer Rights Directive) are robust, they struggle with digital-native harms. Whilst the proposal is not yet public, the Act will likely focus on the following pain points that specifically disrupt the gaming industry's current monetisation and retention models:

- **Addictive Design & Engagement Mechanics:** The Act aims to regulate features engineered to maximise playtime and time-spent-as-payment.
- **Dark Patterns 2.0:** Expanding the DSA's ban on manipulative interfaces to cover all B2C interactions, not just platform interfaces.
- **Personalisation Practices:** The DFA aims to address situations where customer vulnerabilities are targeted for the purposes of personalised advertising and pricing.
- **Minor-Specific Protections:** Implementing a 'fairness by design' standard that assumes a higher degree of vulnerability for younger players, potentially restricting certain types of targeted rewards.
- **Influencer Marketing:** Preventing harmful practices by influencers (e.g. the promotion of harmful products)

On the one hand, the DFA offers a potential path toward a level playing field. If successfully implemented, it could replace the current patchwork of non-binding CPC Principles with a single, streamlined and clear EU regulation, thereby reducing the cost of cross-border compliance. Moreover, stricter fairness rules could be a powerful tool against predatory clones from third-country markets that currently gain an unfair advantage by ignoring European ethical standards. On the other hand, more critical voices argue that the DFA – specifically the rule that would require displaying a real-world monetary value (e.g. euros) for in-game currencies (e.g. coins) – could be frustrating for both game developers and gamers, and even hurt the EU's competitiveness on a global stage. First, European game developers could be forced to develop separate versions of their games for the European market. For smaller European developers, creating a separate version for the European market may not even be financially viable at all. Second, displaying in-

game currencies in a real-world currency would be misleading as it could imply that in-game currencies have real financial value, which is not actually the case. An in-game currency cannot be exchanged, for instance, for euros. Third, the DFA could also undermine the free-to-play model, where users download and play games free of charge and revenues are generated through optional in-game purchases, as this model depends on keeping users engaged in the game and on incentivising them to make voluntary in-game purchases. Fourth and finally, displaying in-game currencies as real-world money could also hurt the gaming experience, through the constant pop-ups prompting approval requests.

Lobbying possible

The DFA has not yet been finalised and there is genuine political uncertainty about whether it will be adopted in its current form. Some Member States (notably Poland and France) have publicly positioned themselves in favour of enforcing existing rules over expanding the regulatory perimeter. Germany could well follow suit, which would materially change the political arithmetic in the Council. The time for resistance is now: lobbying through industry groups (e.g. Video Games Europe) participating in consultations with the Commission and submitting evidence are all effective levers. A key message should be that the EU has not yet fully implemented even the rules already on the books (e.g. the DSA). Layering on further obligations before existing law is bedded in risks undermining legal certainty and the competitiveness of European developers. While resisting the DFA entirely may not be realistic, advocating for a simpler and more consistent legal framework, one that avoids double regulation and preserves sector-specific regimes such as youth-protection law, is certainly worth a shot.

A plethora of obligations – game over for gaming companies?

The Commission is constantly levelling up its consumer protection game. Game developers and publishers now face a plethora of laws and obligations spread across multiple different pieces of legislation. Particularly the DFA will have a significant impact on game developers in Europe as it might require European developers to create a separate European version of their games in order to comply with the Act. As the DFA has not yet been finalised, it is not too late for the gaming industry to push back and lobby against an excess of overbearing rules disguised as consumer protection.

***

BLOMSTEIN will closely monitor further developments and keep you informed. If you have any questions on European Gaming Regulation, Leonard von Rummel, Anna Blume Huttenlauch, Philipp Trube and the entire team are ready to assist you.

BLOMSTEIN | We provide legal support to our international client base on competition, international trade, public procurement, state aid and ESG in Germany, Europe, and – through our global network – worldwide.