International Journal of Scientific Engineering and Science
Volume 9, Issue 9, pp. 64-69, 2025. ISSN (Online): 2456-7361

Compliance-Driven Design: Engineering Age-Appropriate Gameplay under COPPA and GDPR-Kids Regulations

Oleh Riazanov
Head of Game Design, Bini Games, Kitchener, Canada
Email address: oleh.riazanov@gmail.com

Abstract— *The article examines the transformation of the video game design process under a stringent regulatory conjuncture shaped by the updated COPPA, the European GDPR-Kids, and adjacent platform policies. The study aims to develop a systematic methodology for compliance-driven design, in which age verification, data minimization, and verified parental consent are integrated into the game's architecture before writing the first line of code. This applies to the rapid growth of family games, which addresses an exponential risk involving up to 6% of global turnover fines under the DSA, automatic off-boarding from Apple Kids and Google Play Families, as well as eCPM erosion through missegmentation. Novelty, in an interdisciplinary configuration of legal, technical, and sociocultural factors: for the first time in literature, the author juxtaposes the U.S. mixed audience model against the European ban on personalized advertising, extending analysis with the U.K. The Age-Appropriate Design Code, which involves platform filters as the second line of regulatory pressure, proposes a closed safety loop — from a neutral age gate to cryptographically signed consent receipts — thereby reducing legal exposure while maintaining an engaging user experience. The main findings validate that the resilience of the product is not based on post-hoc moderation but rather on proactive mapping of gameplay surfaces, a separate kids' mode, total renunciation of behavioral targeting, and an internalized safe harbor audit in every build cycle. Thus, compliance shifts from a peripheral check to the foundation of engineering thought, where child safety no longer functions as a constraint but as a precondition for competitive advantage. The article will be helpful to game designers, product managers, digital compliance specialists, and scholars of user safety.*

Keywords— *Family gaming, children's data protection, COPPA, GDPR-Kids, DSA, age-appropriate design, compliance-driven game design.*

I. Introduction

The family-gaming market has rapidly accelerated its growth from a novelty to become one of the leading drivers within the industry. In America, participants paid USD 59.3 billion for games in 2024 and 82% of parents who played themselves also regularly played with their children underscoring co-play as a normative family leisure activity [1]. It is also growing elsewhere in the world; Newzoo expects aggregated revenues to reach USD 188.9 billion by 2025, representing a year-over-year increase of 3.4%, despite tentpole releases being delayed and macroeconomic volatility [2]. These figures indicate that the overwhelming majority of major studios cannot ignore underage audiences: games launch simultaneously across dozens of countries, and parents' expectations for child safety are becoming as critical as the balancing of core mechanics.

Errors in handling children's data are now more costly than ever. The updated COPPA, effective April 22, 2025, retained the basic price of a violation: up to USD 53,088 per child whose data were collected without proper consent [3]. In the European Union, the fully effective Digital Services Act (DSA) permits fines of up to 6% of a company's worldwide annual turnover for noncompliance, including breaches of the ban on targeted advertising to minors [4]. The sanctions are not merely financial: Apple explicitly warns that an app placed in the Kids category but violating the rules may be immediately rejected or removed upon any update [5]; Google Play, in turn, specifies that noncompliance with Families Policy may result in removal or suspension without prior notice—and at times the suspension of the entire developer account [6]. In aggregate, these risks render compliance-oriented design not optional but a vital condition of market entry.

II. Materials and Methodology

The study relies on a systematic combination of normative acts, industry analytical reviews, and corporate case studies that illuminate the transformation of design processes under new regulatory constraints. The theoretical base draws from works on the evolution of family gaming and legal frameworks for protecting children's digital safety. According to industry statistics, there is increasing co-play between parents and children [1, 2], while the COPPA amendments and the EU's DSA enforcement newly define economic risks of noncompliance [3, 4]. Other inputs are guidelines of Apple and Google platforms which act not only as mere distributors but also assume a role akin to an independent arbiter regarding acceptable app behavior by technical filters and sanctions that go beyond formal legal provisions [5, 6].

The methodological approach was structured into three sequential analytic blocks. First, a comparative analysis of U.S. and EU law was conducted with emphasis on differences in age thresholds, mechanisms for verified parental consent, and constraints on personalized advertising [7 - 9]. The study also incorporates the U.K.'s Age-Appropriate Design Code, which sets a suite of soft standards that, in practice, shape global data minimization patterns [10], as well as published risk-management practices in the United States that frame age appropriateness as a component of digital health [11].

Second, a systematic review of the policies and technical requirements of the platforms was conducted, these included app stores, advertising SDKs, and user-generated content ecosystems. In particular, Apple's Kids Category and Google Play Families rules were reviewed for their stringent limitations on identifier collection and third-party services that can be used [5, 12], along with cases from monetization providers such as Unity Ads and AdMob that have implemented automatic contextual filters [13]. More focus was also placed on UGC platform policy revisions (e.g., Roblox), wherein multi-layered age controls and content labeling have become mandated.

Then, a content analysis was made of all empirical data on parent perception of digital-environment risk. Surveys have elicited a very high level of concern about the safety of children in games and social networks. Greater unease is found among female parents and the younger cohort of parents [16]. These data were integrated as indicators of social pressure on studios and as corroboration that compliance-oriented design constitutes not only a legal but also a societal imperative.

III. Results and Discussion

The regulatory landscape for designing games for minors is now defined by several acts that entered into force or were updated in 2025, each establishing its own design control points. Their combined effect forces studios to build a safety zone not post-release but at the very first line of code, because misalignment among regional norms promptly triggers store rejections and fines.

Under COPPA, as amended in April, the mixed audience now encompasses any service where children and adults inevitably interact; consequently, a game must determine the age of its users before processing any personally identifiable information. Simultaneously, the regulator expanded the permissible methods for obtaining verified parental consent (VPC): in addition to a traditional micro-transaction, knowledge-based authentication, facial-to-ID matching, and an experimental text-plus method for cases where a child's data is not disclosed are recognized. Eventually, the idea of support to internal operations was formally instructed to be accompanied by a separate notice to parents whenever persistent identifiers are collected—even if they never cross the server perimeter [7]. The European data-protection regime, as Article 8 stipulates, sets the limit at sixteen; Member States may reduce it to thirteen. That is where the responsibility for verification lies, and that is what reasonable efforts entail—on the part of the game service itself. Thus, a global build must dynamically adjust the age threshold based on a player's location and store proof of parental authorization in a machine-readable form for potential supervisory review [8].

Added to this is the DSA, which, from 2025, unconditionally prohibits delivering personalized advertising to minors [9]. Formally, this applies to all platforms, but in practice, mobile games were among the first to lose access to behavioral ad networks: targeting models ceased servicing audiences with unknown or confirmed underage status.

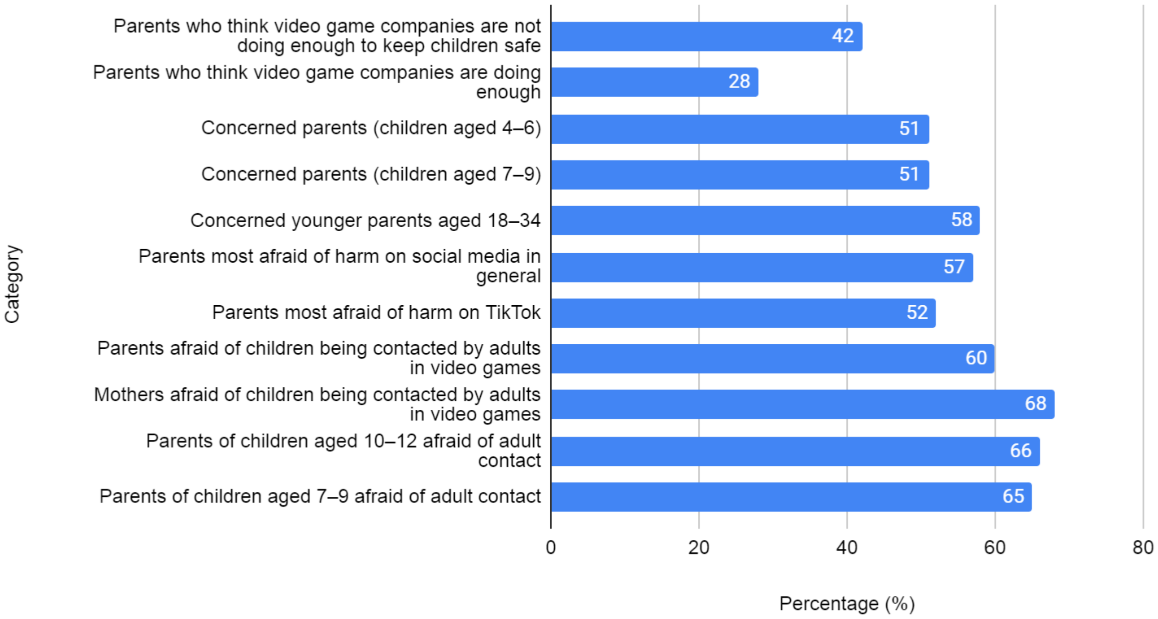

Fig. 1. Parental Concerns on Child Safety in Video Games and Social Media [16]

Outside the direct legislative reach, yet with a profound cross-border influence, sits the U.K. Age-Appropriate Design Code, which articulates fifteen standards in the best interest of the child and effectively bridges the legislative gap between European and American approaches to Data Minimization [10]. High-Privacy Defaults, which it recommends, are already included in risk reviews by major app stores and were published as a set of practices by the U.S. NTIA in 2024, stating that age appropriateness should be considered a user-health component, alongside attention economy concerns [11]. Together, these two documents define soft but influential metrics by which trust-and-safety teams test whether a purported kids' version of a game amounts to more than a cosmetic label. Data in Figure 1 show that parents report high levels of concern about children's safety in the digital environment, especially regarding video games and social networks, with anxieties amplified among younger parents and mothers [16].

Once legal requirements have established a minimally acceptable level of child data protection, actual pressure on studios intensifies through platform rules: app stores and ad intermediaries implement technical filters that render noncompliance practically impossible. Designers can no longer negotiate with a moderator—misconfigured parameters simply fail automated validation, and a game ceases to monetize.

Apple's Kids category exemplifies the strictest model. To gain access, a developer must remove all external links and purchase mechanisms from the child-facing interface, placing them behind a parental gate, and must also forgo third-party analytics and ad SDKs. Any violation yields immediate build rejection during review and potential delisting, making a dual UX with a separate kids' mode mandatory for mixed audiences [5].

The Android ecosystem follows a similar logic with emphasis on identifier control. Google Play's Families policy directly prohibits the transmission of AAID, MAC address, and other unique identifiers for children and users of indeterminate age; apps directed solely to children may not even request AD_ID permission. Additionally, Google requires ad networks to pass the Family Ads SDK self-certification; otherwise, mediation is blocked at the store level. Violations can prompt not only removal of a specific APK but also suspension of the entire developer account, which is why it is safer for designers to engineer contextual-only logic and keep an age flag in app memory without external transmission [12].

Monetization providers have internalized the same philosophy. Unity Ads, by default, treats any user without positive age confirmation as a child and serves only contextual ads; this behavior cannot be altered in a mixed audience, even programmatically, if the project is marked as Mixed Audience [13]. AdMob offers a parallel switch: setTagForChildDirectedTreatment disables interest-based ads and remarketing, forcing untargeted delivery. Thus, even if client logic errs, the ad stack insulates the developer from violation—but at the cost of lower eCPM, creating incentives to determine age more precisely and segment ad inventory within the game itself.

UGC platforms have gone further, introducing multi-layer access stratification. In 2024, Roblox required developers to age-rate all experiences, closed under-13 access to unrated projects, and in 2025 began blocking games entirely if the author failed to set a rating; such projects remain developer-only until they pass review [14]. Entry to the 17+ section requires identity verification via an official document scan, effectively mirroring one of the new VPC methods but aimed at adults. Similar mechanisms are being gradually adopted by other UGC services, making content metadata and age gates mandatory elements of the publication pipeline [15].

The sum of these platform constraints forms a second, stricter control line atop the law: even a formally compliant but technically misconfigured game can no longer pass review, monetize, or remain available to its audience. Accordingly, conformance with store and SDK-partner rules is not a peripheral add-on to legal analysis but an integral component of game design that determines data architecture and the project's economic viability.

The foundation for a safe game is laid before the first level exists: at specification time, the developer must stratify the audience by age and construct a neutral gate that, in a non-coercive manner, ascertains age before the client touches any personal byte. Such a gate neither tempts a child to game the flow nor signals that adult status is inherently valuable, statistically reducing false responses. It also serves as the technical branching point: if age is below thirteen, the game activates a protected profile in which all requests for personal information are immediately blocked.

Data minimization follows. Rules and stores allow the retention of persistent identifiers solely for internal telemetry, fraud control, and frequency capping purposes. Therefore, any field not fitting this triad should disappear from the model by default. Best practice is to define the whitelist of permitted purposes in server configuration and make client transmission contingent on this table rather than on an analyst's desire for another parameter. The shorter the list, the less often a game attracts formal claims.

Monetization for child and indeterminate segments can now rely only on context. For developers, this means the ad stack should decide based on scene genre, time of day, and frequency limits—but never on behavioral history. Regulatory safety offsets eCPM losses: the project avoids strikes in personalized advertising and abrupt network cut-offs that have occurred in games relying on behavioral profiles. Parental consent onboarding turns short and elastic, not in the form of a tedious, long paper. The interface must present at least two options — knowledge-based questions and swift biometric face-to-document matching. Text confirmation is only good where the game discloses zero child data. The pick remains with the adult; the game records only the fact of successful verification and its validity period, without storing any raw biometric material.

The project will embed safe-harbor audits directly into the build pipeline. Each major update passes an internal checklist, cross-checked against platform rules, and, if required by external auditing, is reviewed before being uploaded to the store. This serves to discipline the team. When a violation is found in the closed testing channel, remediation is cheaper than a public build recall or even a fine.

Consent must outlive any particular client version. A receipt is made in an international profile, cryptographically signed, and stored as a portable artifact. When a child moves to a different platform or the studio changes its infrastructure, the consent token travels with the profile- no more re-entering identity documents, and no more data bloat. The loop from the neutral gateway back to durable proof in Figure 2 closes: all elements reinforce one another to reduce legal risk while maintaining smooth gameplay.

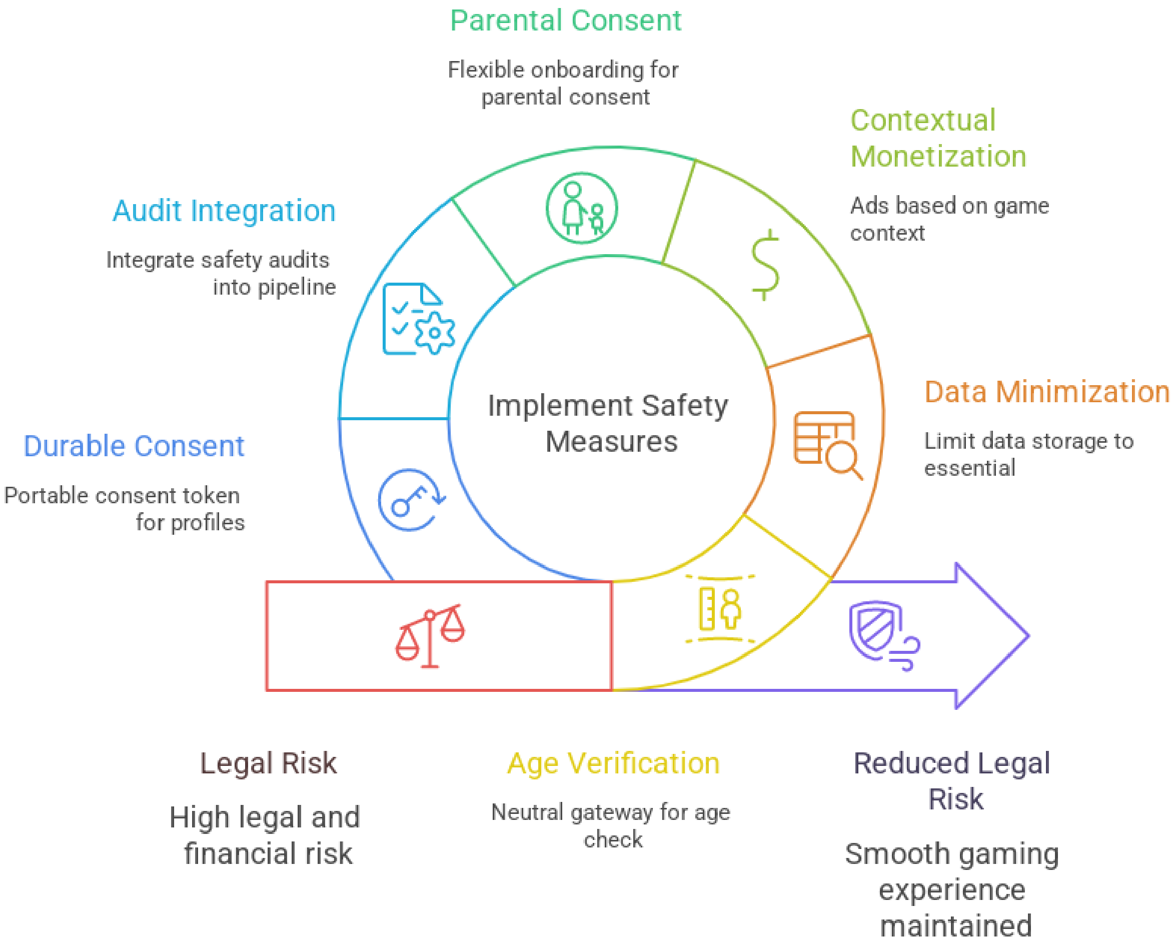
Parental Consent
Flexible onboarding for parental consent
Contextual Monetization
Ads based on game context
Audit Integration
Integrate safety audits into pipeline
Implement Safety Measures
Data Minimization
Limit data storage to essential
Durable Consent
Portable consent token for profiles
Legal Risk
High legal and financial risk
Age Verification
Neutral gateway for age check
Reduced Legal Risk
Smooth gaming experience maintained

Fig. 2. Loop for Building a Safe Gaming Environment

Begin by breaking down every scene and interaction type into three archetypes: child, mixed, and general. The child archetype encompasses any locations where a child might inadvertently leave personal traces. Mixed spaces are those in which children and adults interact side by side- they generally comprise zones without real risks of disclosure. This cartography is completed at the whiteboard and then recorded in the server configuration. At runtime, the client requests the current surface type and conforms its behavior such that if a scene is marked as a child, personal chats, web links, and identifier collection are simply disabled with no further checks.

A dedicated kids' mode is then created. This is not a pared-down clone of the main game, but an autonomous set of activities tailored to constraints on communication and payment. Only single-player or tightly scripted co-op missions are permitted; the interface contains no outbound links; and in-app purchases are placed behind a parental gate. The mode runs in parallel with core content, switching instantly as the player's age status changes, sparing the product from issuing a separate build.

The next layer is ad logic. The ad module runs in strictly contextual mode: selection depends on level genre, time of day, and a frequency cap, never on behavioral history. The cap is enforced as a hard server policy, preventing chaotic repetition of creatives. If age is unconfirmed, the module automatically inherits the same settings as for a child profile; thus, mixed audiences receive identical protection until the user completes age verification.

To confirm a child's right to be in the game, the interface offers at least two parental-consent channels: knowledge-based questions and a quick biometric check against an ID. The user selects the convenient option; the system stores only the success marker and expiration time. Text confirmation is available solely in modes where the game fundamentally does not disclose personal data, and this is clearly stated in the dialog.

Each successful consent session finally issues a cryptographically signed attestation. It is stored server-side together with a machine-readable receipt suitable for transfer across applications. During account migration or database moves, the token travels with the profile, eliminating the need for repeat document checks. The internal audit periodically reconciles attestation validity and automatically initiates re-authentication as the expiry approaches. The resulting architecture is shown in Figure 3.

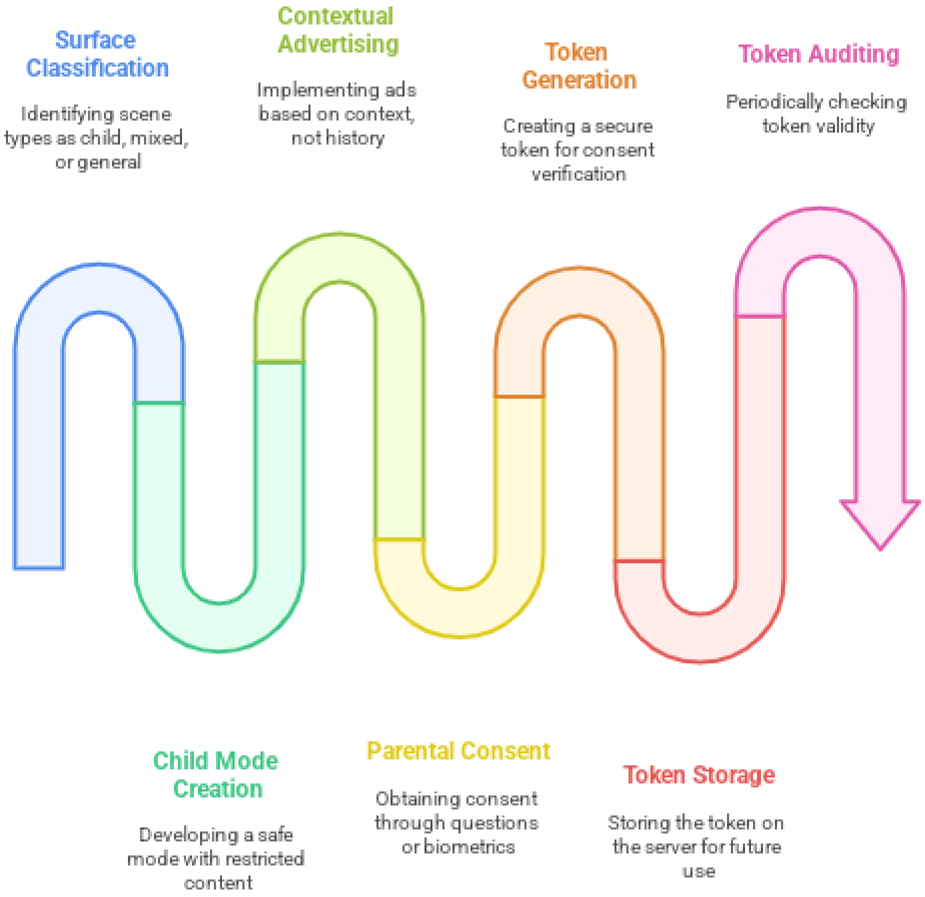
Surface Classification
Identifying scene types as child, mixed, or general
Contextual Advertising
Implementing ads based on context, not history
Token Generation
Creating a secure token for consent verification
Token Auditing
Periodically checking token validity
Child Mode Creation
Developing a safe mode with restricted content
Parental Consent
Obtaining consent through questions or biometrics
Token Storage
Storing the token on the server for future use

Fig. 3. Game Safety and Consent Process

In this way, the whole cycle closes: surface classification governs client behavior; kids' mode guarantees safe content; contextual advertising eliminates profiling; flexible consent lowers entry friction; and durable receipts ensure verifiability even years later.

IV. Conclusion

The evolution of family gaming and a stringent regulatory milieu relocates compliance from the periphery to the core of the design process. Whereas child protection against unwanted content and unlawful data collection used to be addressed post-factum, it is now integrated into the game's architecture from the outset. It has been shown that legal acts—such as the updated COPPA, the EU data-protection regime, and the DSA—collectively create a mandatory design contour in which every mechanic, every interface element, and every ad integration must be rethought through the prism of compliance.

Further analysis demonstrated that pressure is intensified not only by oversight bodies but also by distribution and monetization platforms themselves, turning technical correctness into a precondition for economic viability. The practical steps—surface classification, a distinct kids' mode, a pivot to contextual advertising, flexible parental-consent flows, and durable receipts—cohere not as isolated measures but as a unified design framework. It is precisely this integration that aligns legal, technical, and user logics, reducing sanction risk while preserving the appeal of play.

Accordingly, the study demonstrates that compliance-oriented design has established a new standard of engineering thought in the industry. It unifies regulatory constraints, parental interests, and children's expectations into a coherent system in which safety is not opposed to engagement but becomes its foundation.

References

[1] "2025 Essential Facts About the U.S. Video Game Industry," *ESA*, Jun. 03, 2025. https://www.theesa.com/resources/essential-facts-about-the-us-video-game-industry/2025-data/ (accessed Jul. 31, 2025).

[2] Z. Kachwala, "'GTA VI' delay weighs on global videogame market growth, data shows," *Reuters*, Jun. 17, 2025. Accessed: Aug. 01, 2025. [Online]. Available: https://www.reuters.com/business/media-telecom/gta-vi-delay-weighs-global-videogame-market-growth-data-shows-2025-06-17/

[3] Federal Trade Commission, "Complying with COPPA: Frequently asked questions," *Federal Trade Commission*, 2025. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (accessed Aug. 02, 2025).

[4] European Commission, "Questions and answers on the Digital Services Act," *European Commission*, Nov. 14, 2022. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 (accessed Aug. 03, 2025).

[5] Apple Developer, "App Store Review Guidelines," *Apple Developer*, Sep. 13, 2024. https://developer.apple.com/app-store/review/guidelines/ (accessed Aug. 04, 2025).

[6] "Developer Program Policy," *Google*, 2025. https://support.google.com/googleplay/android-developer/answer/16543315?hl=en (accessed Aug. 05, 2025).

[7] "Children's Online Privacy Protection Rule," *Federal Register*, Apr. 22, 2025. https://www.federalregister.gov/documents/2025/04/22/2025-

05904/childrens-online-privacy-protection-rule (accessed Aug. 06, 2025).

[8] "Regulation (EU) 2016/679," *Official Journal of the European Union*, vol. L119, no. 1, Accessed: Aug. 07, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679

[9] European Commission, "The impact of the Digital Services Act on digital platforms," *European Commission*, Nov. 03, 2023. https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms (accessed Aug. 08, 2025).

[10] E. Denham, "Age appropriate design: a code of practice for online services," *ICO*, May 19, 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ (accessed Aug. 09, 2025).

[11] "Industry's Role in Promoting Kids' Online Health, Safety, and Privacy: Recommended Practices for Industry," *NTIA*, 2024. https://www.ntia.gov/report/2024/kids-online-health-and-safety/online-health-and-safety-for-children-and-youth/taskforce-guidance/recommended-practices-for-industry (accessed Aug. 10, 2025).

[12] Google, "Google Play Families Policies," *Google*. https://support.google.com/googleplay/android-developer/answer/9893335?hl=en (accessed Aug. 11, 2025).

[13] "Child data law compliance, CARU compliance, and contextual ads," *Unity*. https://docs.unity.com/en-us/grow/ads/privacy/coppa-compliance (accessed Aug. 12, 2025).

[14] Roblox, "Age ID Verification," *Roblox*. https://en.help.roblox.com/hc/en-us/articles/4407282410644-Age-ID-Verification (accessed Aug. 13, 2025).

[15] A. Shearon, "Roblox makes unrated games inaccessible starting next month, has a plan for old favorites to ensure these cherished classics are not lost," *PC Gamer*, 2025. https://www.pcgamer.com/games/roblox-makes-unrated-games-inaccessible-starting-next-month-has-a-plan-for-old-favorites-to-ensure-these-cherished-classics-are-not-lost/ (accessed Aug. 30, 2025).

[16] "Playsafe ID survey reveals 42% of parents say game studios fail to protect kids online," *Game Industry News*, 2025. https://mobidictum.com/playsafe-id-survey-game-studios-online-protection/ (accessed Aug. 15, 2025).