

Eurochild's reaction to the proposed EU KIDS Act



Eurochild
Putting children at
the heart of Europe

October 2026

Eurochild's reaction to the proposed EU KIDS Act

Introduction

Eurochild welcomes the proposed EU KIDS Act as a necessary step to strengthen children's rights and hold providers accountable in the digital environment. It builds on the protections provided by the Digital Services Act (DSA), General Data Protection Regulation (GDPR), AI Act and consumer law, whose effective enforcement remains essential, and complements them with safeguards adapted to children's development. We welcome the move to establish binding safety-by-design requirements, also building on protections set out in the DSA Guidelines on the protection of minors and strengthening providers' accountability for children's online experiences.

As recognised in the Special Panel co-chairs' [report](#), published in July, to which Eurochild also contributed, children's needs, capacities and vulnerabilities change throughout childhood and adolescence. Digital services should reflect their physical, cognitive, emotional and social development, supporting their growing autonomy and opportunities to learn, connect, seek support and participate. This approach is grounded in the UN Convention on the Rights of the Child, ratified by all EU Member States, and Article 24 of the EU Charter of Fundamental Rights, which recognises children's rights, views and best interests.

By establishing binding safety-by-design requirements across the covered services, the EU KIDS Act can help ensure that children's rights in the digital environment do not depend on their family's resources or access to guardian support. Alongside strong consumer protections and the forthcoming Digital Fairness Act, it offers an opportunity to address harmful design and commercial practices. During negotiations, Eurochild will advocate for necessary, proportionate and effective measures that enable all children, particularly those in vulnerable situations, to enjoy their rights safely and increasingly independently.

What Eurochild welcomes

The broad scope - We welcome coverage including online social networking services, video-sharing platform services, software application stores, online games, operating systems, AI companions and general conversational chatbots, as well as the absence of a general exemption for small and micro providers.

Article 3 - Definition of minor or child: We welcome the clear definition of a child as any person under the age of 18, ensuring that the Regulation recognises the rights of children throughout childhood.

Article 4 - Anti-circumvention: We welcome the prohibition on providers engaging in any behaviour that undermines or circumvents their obligations, including through interface design and behavioural techniques.

Article 5 - Compliance plans and independent audits: We welcome the requirement for providers of social networking and video-sharing services designated as very large online platforms to submit compliance plans for independent audit, including expertise in children's rights.

Article 8 - General obligations on safety by design: We welcome the binding obligation for social networking services, video-sharing platforms, online games, AI companions, general conversational chatbots and software application stores to ensure a high level of privacy, safety and security for minors. These providers must apply the safety-by-design requirements of Chapter III by default, including where services are used without an account, and may only derogate from those requirements after establishing, through age assurance, that the user is an adult.

Article 9 - Addictive design: We welcome the prohibition on designing, organising or operating services in ways intended, or reasonably foreseeable, to encourage compulsive or excessive use by minors. This includes autoplay and uninterrupted content consumption without effective, regular stopping points; notifications that undermine children's decisions to stop using the service; and incentives or penalties that encourage frequent or repeated engagement. We also welcome requirements for effective time-limited access and interruptions of use that protect school time and core sleep hours.

Article 10 - Recommender systems: We welcome specific safeguards for recommender systems used by minors, including requirements not to exploit children's vulnerabilities or attention, to prioritise explicit preferences, to disable recommendations based on implicit engagement signals from children's online behaviour by default and to provide an option that is not based on profiling.

Article 11 - Safe settings: We welcome the requirement for high privacy, safety and security settings by default, including turning off geolocation and tracking, camera and microphone access, account recommendations and push notifications by default. It is also positive that features posing risks to children's privacy, safety, health or well-being must not be made available to minors.

Article 12 - Contact and interaction safeguards: We welcome strong protections around contact with other users, including restrictions on unsolicited contact, contact recommendations and group additions, as well as stronger default protections for the visibility of children's content and personal information.

Article 13 - Safety and security of economic transactions: We welcome safeguards against the exploitation of children's developing commercial literacy, including clearer information about economic transactions and measures preventing excessive, impulsive or unwanted spending and exposure to variable-reward systems.

Article 14 - Obligations for AI companions and general conversational chatbots: We welcome safeguards against addictive design and emotional dependency, safe default settings, and testing before market placement or deployment. We also welcome post-market monitoring, while noting the exemption from this specific duty for micro and small enterprises. Where these AI systems are embedded in social networking services, video-sharing services or online games, they must not activate automatically or be prominently displayed; minors must not be encouraged to use them and must be able to opt out easily.

Article 15 - Obligations for providers of online games: We welcome the inclusion of online games within the safety-by-design framework, including safeguards on addictive design, safe settings and contact risks in online games.

Articles 16 and 17 - Obligations for age-appropriate access: We welcome the inclusion of app stores in the Regulation, the requirement for age-rating systems, and the obligation to prevent minors from accessing or purchasing applications inappropriate for their age. We also welcome public information on rating methods and cooperation through codes of conduct to achieve more consistent ratings, while leaving room to strengthen consistency at key age thresholds.

Article 18 - Agency of minors: We welcome the requirement to provide children with accessible tools to control content, settings and recommendations, helping to strengthen their agency within digital services.

Article 19 - Child-friendly reporting and support tools for minors: We welcome the requirement for child-friendly and easily accessible reporting mechanisms, priority handling of reports submitted by minors, and information for children about the procedure followed and available redress.

Article 20 - Tools for guardians: We welcome the requirement for accessible and easy-to-use tools that can help guardians support children's online experiences. Such tools can be useful when they complement providers' own safety obligations and respect children's evolving capacities. We also welcome safeguards for children's privacy and agency, including informing children when guardian tools are being used.

Article 21 - Collective complaints: We welcome children's and guardians' right to mandate eligible not-for-profit bodies, organisations or associations to exercise children's rights on their behalf, alongside the right of children, guardians and eligible organisations to lodge complaints alleging infringements concerning social networking services, video-sharing platform services, video gaming platforms, AI companions and general conversational chatbots.

Article 22 - Monitoring obligations for providers of very large platforms: We welcome the requirement for providers of covered services designated as very large online platforms to monitor, test and evaluate the effectiveness of their protective measures.

Articles 25 and 39 - Adaptation to evolving challenges: We welcome the possibility of adapting specified safety-by-design requirements to scientific and technological developments through delegated acts, subject to the limits and safeguards governing those powers.

Articles 27 and 28 - General principles of age assurance: We welcome strong safeguards around age assurance, including requirements for accuracy, reliability, security, robustness, non-intrusiveness, privacy, data protection and non-discrimination. It is particularly positive that age-assurance solutions must not enable identification, location, tracking, targeting, advertising or profiling, and that personal-data processing must be limited to what is strictly necessary. We also welcome Article 28(3), which states that any age-assurance measure shall be a zero-knowledge proof.

Article 29(6) - Sharing of age signals through operating systems: We welcome the requirement that, where an operating-system provider has already obtained an age signal through age assurance meeting Article 27's requirements, it must, with the user's consent, enable that signal to be shared with providers where necessary for compliance with the Regulation. This can support interoperable, privacy-preserving age assurance and help avoid repeated age checks while limiting unnecessary data processing.

Article 35 - Expedited procedure: We welcome expedited Commission enforcement proceedings for designated very large online platforms and AI systems under its exclusive supervision, including the obligation to endeavour to adopt a final decision within 90 working days of opening proceedings.

General principles to strengthen in the proposal

One coherent safety-by-design framework: Ensure equivalent core protections across digital services, with additional safeguards tailored to their specific risks and aligned with other EU legislation.

Reverse the burden of proof: Require providers to demonstrate safety and age-appropriateness before exposing children to services, supported by child-rights risk assessments and independent review. Make child rights assessments and proportionate independent review conditions for market access for services offered to minors, requiring providers to implement safeguards and justify permitted age ranges before offering those services to children. They should also continuously evaluate the safety and age-appropriateness once exposed to children, and evaluate new features and functionalities being introduced.

Protection independent of guardian availability: Ensure children's rights and basic safeguards do not depend on adults' availability, resources or digital skills. Accommodate diverse family structures and care arrangements.

Inclusion and accessibility by design: Remove barriers and assess unequal impacts through a gender-sensitive and intersectional approach, prioritising children in vulnerable situations and ensuring safeguards are usable in practice.

Children’s agency, privacy and evolving capacities: Support autonomy, independent learning and confidential access to help, while preventing harmful dependency, excessive use and disproportionate monitoring.

Meaningful participation and independent accountability: Involve children in designing, testing, and reviewing safeguards, alongside independent expertise, ongoing research, effective complaints, and evaluation of real-world outcomes.

Public support for equitable implementation: Invest in digital literacy, support for families and educators, and shared, accessible, privacy-preserving infrastructure so that effective protection is available across services and communities.

Our paper on how children’s backgrounds shape their rights in the digital environment further highlights why safeguards must account for inequalities in access, exposure to risks and the support available to children.

Specific recommendations by article

Article 2 - Scope and educational services

Article 2 determines the scope of the Regulation. It excludes specified categories of services and systems, including those designed for primarily educational purposes and operated by educational establishments or organisations, or on their behalf.

The educational exemption should be limited to services and systems designed and operated exclusively for educational purposes, replacing ‘primarily educational purposes’ in Article 2(4)(c). The Regulation should establish clear criteria for applying the exemption, so that providers cannot avoid their obligations simply by describing a service as educational. This exemption should be limited to services demonstrated, through a proportionate risk assessment, to pose very low risks to children. Exemptions should not create loopholes or leave children without appropriate protection when evidence shows risks, while obligations should remain proportionate for legitimate educational and small-scale providers. Regardless of this exemption, educational conversational AI accessible to children should remain subject to the relevant protective obligations, while being exempt from the proposed minimum-age access restriction.

Article 3 - Definition of guardian

The proposal defines a guardian as a person holding parental responsibility under national law and relies on guardians for certain accounts, access arrangements and controls.

Article 3(5)(b) should explicitly accommodate legally authorised institutions, bodies and professionals exercising parental responsibility, drawing on the definition in the Brussels IIb Regulation. The framework should also clarify how legally appointed representatives of

unaccompanied children can support access and exercise relevant functions within their lawful mandate, where that mandate does not amount to parental responsibility under national law. Appropriate cross-references to the Asylum Procedures Regulation and Reception Conditions Directive should ensure that these arrangements accommodate the circumstances of unaccompanied children and do not create barriers to their access, protection or confidential support.

Article 3 - Common definition of safety by design

The proposal includes a Chapter III titled “Safety by design”, and Article 8 imposes a general obligation to ensure a high level of privacy, safety, and security for minors by default. Still, Article 3 does not define “safety by design” as a legal concept.

The Regulation should introduce a clear, common and technology-neutral legal definition of “safety by design”. The definition should establish that providers must identify, prevent, and mitigate risks to children’s rights, safety, privacy, health, well-being, and development from the earliest stages of a service or system’s design and development and throughout its lifecycle. It should apply consistently across technologies and service categories within the Regulation’s scope, and require protective measures to be embedded by default, rather than relying primarily on children or guardians to manage risks after they arise.

Article 3 - Definition of services and systems accessible to minors

Article 2(1) applies the Regulation to specified services and systems “accessible to minors”, but Article 3 does not expressly define this concept. DSA recital 71 and the Commission’s guidelines provide relevant interpretative criteria for online platforms.

The Regulation should expressly define “accessible to minors” in its operative provisions, building on those criteria and adapting them to all service and system categories within its scope. In line with DSA recital 71 and the Commission’s guidelines under Article 28 of the DSA, the definition should cover circumstances where providers permit access by minors, where services or systems are directed at or predominantly used by minors, or where providers know or can reasonably be expected to know that minors use them. A statement in the terms and conditions prohibiting children’s access should not, by itself, exclude a service or system from the Regulation’s scope where effective measures to prevent that access are absent.

Article 3 - Educational AI and the definition of general conversational chatbot

Article 3(5)(d) excludes AI systems whose conversational functionality is limited to specialised services, tasks or predefined functions, including specialised educational applications, from the definition of a general conversational chatbot.

The Regulation should ensure that this definitional exclusion does not leave children using educational AI without relevant protection. Articles 2, 3 and 14, together with related provisions, should be amended coherently to expressly cover educational conversational AI accessible to children for protective purposes, whether provided independently or embedded in an educational service. This could be achieved through a separate category, without treating specialised educational systems as general conversational chatbots. The

targeted exemption from age-based access restrictions should remain distinct from providers' protective obligations.

Article 5 - Compliance plans and independent audits

Article 5 requires compliance plans and independent audits for social networking and video-sharing services designated as very large online platforms. It does not establish the same procedure for standalone AI companions, general conversational chatbots or online games. Article 14 requires pre-market evaluations and testing, but does not expressly require these to be independent.

Audits should meaningfully assess whether proposed safeguards can protect children in practice, with effective implementation and verification of corrective measures where shortcomings are identified. Proportionate independent scrutiny should extend beyond the platforms covered by Article 5 to AI companions, general conversational chatbots, and online games where their risks to children warrant it.

Auditors should be selected or approved by the competent supervisory authority under transparent criteria, with safeguards against conflicts of interest. Audits should test whether safeguards work in practice, including whether interface design, repeated prompts or other engagement techniques undermine time limits, interruptions and protections for school time and sleep.

Article 6 - Delayed creation and use of accounts

Article 6(2) allows guardians to establish limited accounts for children aged 13 or over and under 15 on the social networking and video-sharing services covered by Article 6(1). It requires guardian tools to remain activated and enables guardians to set a daily access limit not exceeding one hour, pre-approve potential new contacts and set a maximum number of contacts. Article 6(3) requires providers to establish the account creator's parental responsibility and verify the child's age eligibility.

We recommend amending Article 6(2)-(3) so that, from age 13, children can hold a limited account in their own right, without its creation or continued use depending on an available guardian. Limited-account safeguards should remain binding, with providers responsible for implementing them independently of guardian involvement:

- **Article 6(2)(a) - Optional guardian tools:** Replace the requirement for continuous activation with a requirement that tools remain available for optional use. Their activation should neither determine access to the account nor be necessary for its basic protections.
- **Article 6(2)(b) - A built-in daily limit of one hour:** Require providers to apply this limit automatically. Guardians could set a shorter limit through optional tools, taking into account the child's needs, views, and evolving capacities. The Regulation should clarify that the daily limit applies cumulatively within each service category: a maximum of one hour across all social networking services and a separate maximum of one hour across all video-sharing platform services, rather than one hour per platform. Time limits should distinguish between functions and purposes of use. Narrowly defined essential

functions, such as direct calls with family and friends, confidential access to support and necessary assistive uses, should remain available when the limit is reached and should not count towards it. These exceptions should not enable continued access to feeds, recommendations or other engagement features. Implementation should preserve privacy without monitoring private communications and should not depend on guardian authorisation.

- **Article 6(2)(c) - Safe contacts and a proportionate contact limit:** Require providers to apply restrictions on unsolicited contact, age-appropriate safeguards for adding new contacts and a proportionate maximum number of contacts. Guardian pre-approval could be an optional additional safeguard, while children without an available guardian should still have a safe way to establish legitimate contacts. Unsolicited private messages should not be allowed.
- **Related provider safeguards:** Ensure limited accounts retain high privacy and security settings by default, protections against harmful recommendations and addictive design, and accessible blocking, reporting and confidential support tools that children can use independently, building on Articles 8-12 and 18-19. For limited accounts for children aged 13-14, these additional safeguards should include:
 - Prohibition of addictive features. Providers should be mandated to turn off short-form video feeds and sequential ephemeral-content features, such as Shorts, Reels and Stories.
 - Behavioural profiling should always be prohibited.
 - Public livestreaming should remain unavailable.
 - The child's account and content should not be visible to users outside the child's approved contacts.

Article 6(3) - Separate account creation from guardian verification: Retain age verification, but require verification of parental responsibility when an adult activates guardian tools, rather than making it a prerequisite for the child's account.

Consequential amendments to Article 6(4) and related provisions, including Articles 26 and 29 where necessary, should ensure consistency with child-held limited accounts. Eligible existing accounts should be retained or converted into compliant limited accounts, and verification of parental responsibility should be required when guardian tools are activated rather than as a condition for creating or continuing to use the child's account. Independent creation and use of limited accounts should be distinguished from parental consent to personal data processing where required under Article 8 of the GDPR. Providers should clearly explain when such consent is necessary, without treating it as authorisation for guardian monitoring or control.

Overreliance on parents and guardians risks making children's access and protection depend on adults' availability, digital skills, resources and capacity to provide support. These vary considerably, and some children have no available guardian or cannot safely rely on the adults responsible for them. Mandatory guardian control could therefore deepen inequalities, exclude children, restrict their privacy and access to confidential support, and

create inconsistent restrictions or delays in establishing legitimate contacts. It may also place an unreasonable burden on families to manage risks that providers should address through service design.

This is particularly important for children in alternative care and children with a migrant background, including unaccompanied children, who may rely on digital services to maintain family contact, access information and seek support with family reunification. Their account, established contacts and access to support should remain with them through changes in care arrangements or location.

The proposed amendments should build on Article 18's recognition of children's agency and Article 20(1)(e)-(f) and (2), which require guardian tools to avoid disproportionate restrictions on children's rights, respect their agency and privacy, and inform children when tools are used. Optional guardian tools should support these principles: their use should be transparent to the child, proportionate, responsive to children's needs, views and evolving capacities, and preserve confidential access to helplines and support services. This recommendation builds on recital 43's recognition that guardians may be absent or disengaged and that compliance should not depend exclusively on them.

Article 7 - Child-specific video-sharing services for children under 13

Article 7 allows children aged 3-12 to access child-specific video-sharing services through a guardian-established account, with access enabled and controlled through guardian tools.

The Regulation should require providers to demonstrate that child-specific video-sharing services are suitable for the ages they serve. Building on the published assessment required by Article 7(1)(d), the Regulation should require a comprehensive child-rights risk assessment and proportionate independent review demonstrating suitability for the ages served before access is allowed. The minimum age of three should remain a lower boundary, rather than a presumption that a service is suitable for every child above that age.

Access for children aged 3-12 should remain organised through a guardian-held account, as provided for in Article 7, with child-specific profiles or settings adapted to the child's age and evolving capacities. Providers should apply binding safety-by-design safeguards automatically, without requiring guardians to configure or activate each protection. Guardian tools should provide additional support while respecting children's privacy and agency. The Regulation should accommodate diverse lawful care arrangements and changes in guardianship, ensuring that children in alternative care and other vulnerable situations are not excluded because standard parental arrangements or documentation are unavailable.

The Regulation should expressly clarify that the exception cannot be used to circumvent Article 6 by presenting a service combining video-sharing and social-networking functions as a child-specific video-sharing service. Eligibility should depend on the service's actual design. The exception should be limited to age-appropriate video-viewing environments, with narrowly defined ancillary functions, and should not permit social-networking features that recreate the risks underlying the access restrictions.

Article 9 - Addictive design

Article 9 prohibits design that encourages compulsive or excessive use and requires measures for time-limited access and interruptions. It addresses features such as autoplay, notifications not triggered by or not related to the minor's interaction or activity on the service, and incentives to return regularly.

The Regulation should clarify how these obligations apply to other practices that may pressure children to remain online or return, including repeated prompts, social proof, urgency cues, read receipts and typing indicators. Risk assessments should consider the cumulative effect of several design features rather than assessing each feature separately, and how certain groups of children, such as children with disabilities, including children with autism, might be impacted by them.

Articles 9(3), 15 and 20 - Time limits and interruptions in online games

Article 14 expressly incorporates Article 9(3) for AI companions and general conversational chatbots, whereas Article 15 does not directly incorporate it for online games. Article 20 nevertheless requires time-management mechanisms within guardian tools, so the proposal does not leave gaming time limits entirely unaddressed.

Article 15 should expressly require providers to implement effective time-limited access and interruptions of play, designed to protect children's school time and core sleep hours. These safeguards should operate independently of guardian involvement, while accommodating accessibility needs and assistive uses.

Article 10 - Recommender systems

Article 10 establishes safeguards for recommender systems used by minors on social networking and video-sharing services, including prioritising explicit preferences, disabling recommendations based on implicit engagement signals by default, and providing a non-profiling option.

Providers should explain to children what their recommender systems optimise for and how engagement and commercial objectives are weighed against safety, quality and wellbeing. The metrics used to assess children's safety and wellbeing should be open to meaningful independent scrutiny. Article 15 should expressly extend equivalent recommender-system safeguards to online games and gaming platforms. Recommendations of games, experiences, content or further interactions should not exploit children's vulnerabilities or optimise engagement at the expense of their rights and well-being.

Articles 10 and 14 - Equivalent safeguards for AI recommendations

Article 14 does not expressly extend the recommender-system safeguards in Article 10 to AI companions and general conversational chatbots.

Where these AI systems recommend content, activities or further interactions, equivalent safeguards should apply to their recommendation functions. Providers should prioritise children's explicit preferences, avoid exploiting their vulnerabilities or attention, and disable

recommendations based on implicit engagement signals by default. Children should have accessible tools to understand, control and reset personalisation.

Articles 11 and 15 - Changes to safe settings and exclusion of harmful features

Article 14 incorporates Article 11 for AI companions and general conversational chatbots, whereas Article 15 expressly incorporates only Article 11(1) for online games. It does not expressly extend Article 11(2)'s conditions for changing defaults or Article 11(3)'s exclusion of harmful features.

Online games should provide equivalent safeguards governing changes to default settings and preventing children's access to features that pose risks to their privacy, safety, security, health or well-being. Any permitted changes should be subject to equivalent age conditions, clear information and explicit consent. Geolocation and other tracking features enabled by children should switch off when their session ends.

Articles 12 and 15 - Contact risks on online games

Article 15(1)(c) extends only selected Article 12 safeguards to online games: Article 12(1), covering pre-approved direct contact, exclusion from contact recommendations, explicit agreement before group additions and easy blocking; and Article 12(3)(c), prohibiting disclosure or sharing of children's personal contact details with other users. It does not expressly extend Article 12(2), protecting children against manipulation into approving contact, or Article 12(3)(a)-(b) and (d)-(f), covering privacy and visibility settings, restrictions on downloading and capturing children's information and content, and livestreaming disabled by default.

All Article 12 safeguards should apply to online games, including protection against manipulation into accepting contact; private account information and content by default; control over the visibility of content, interactions and metrics; restrictions on downloading and capturing children's information and content; and livestreaming disabled by default. Protection against enticing children into risky contact on other services should also extend across all relevant services.

Articles 13 and 15 - Monetisation and gaming

Article 13 prohibits exposing minors to variable-reward systems on social networking and video-sharing services, including purchases made with virtual currency. However, it does not expressly extend that prohibition to online games. This is despite Recital 40 stating that minors playing online games should receive the same level of protection for economic transactions.

The Regulation should prohibit providers from offering paid loot boxes and other purchasable randomised rewards to minors in online games, including where payment is made through virtual currency or an intermediary purchase. It should also require safety settings and safeguards against other monetisation practices that encourage excessive, impulsive or unwanted spending. Child-specific safeguards on economic transactions should complement existing consumer law and the forthcoming Digital Fairness Act, with clear coordination to address gaps and avoid inconsistent obligations.

Article 13 - A pause before purchases

Article 13 prohibits design that leads to excessive, impulsive, or unwanted spending, but it does not expressly require a separation or pause before a purchase.

The Regulation should require proportionate, age-appropriate friction before purchases, including a clear confirmation step displaying the real monetary cost and an opportunity to reconsider. These safeguards should support deliberate choices, particularly for repeated purchases or purchases using virtual currency, remain accessible and avoid pressure to complete the transaction.

Where prices are expressed in virtual currency, providers should display the equivalent real-money cost clearly alongside them throughout the purchasing process, including before confirmation. Children should not have to calculate exchange rates or navigate several currency conversions to understand what they are spending.

Article 14 - Minimum age for access to AI companions and conversational chatbots

Article 14(1)(d) requires that access for children under 13 be enabled and controlled through guardian tools, without setting a lower minimum age. Article 3(5)(d) excludes from the definition of a general conversational chatbot AI systems whose conversational functionality is limited to a specialised service, task or predefined set of functions, including specialised educational applications.

Providers should not enable children under 13 to access AI companions or general conversational chatbots. This restriction should not prevent children from accessing specialised educational AI whose conversational functionality is limited exclusively to educational purposes and which does not otherwise qualify as an AI companion. Their exclusion should not, however, be treated as evidence of safety or age-appropriateness.

A minimum age of 13 should not be treated as evidence that AI companions or general conversational chatbots are suitable for children aged 13-17. Providers should demonstrate age-appropriateness through an independent child-rights risk assessment and testing before access is permitted. Systems and functions that cannot meet this standard should remain unavailable to minors.

Persistent conversational memory should be disabled by default for minors. Any permitted activation should be subject to age-appropriate safeguards and clear information about what is retained and why. Children should have accessible controls to view and delete retained information. Providers should not use that information to exploit vulnerabilities, deepen emotional dependency or pressure children to continue interacting.

Improved guardrails should not, in themselves, justify an exception to the proposed prohibition on access for children under 13. For children aged 13-17, providers should demonstrate age-appropriateness before permitting access.

Specialised educational AI excluded from the definition of a general conversational chatbot should nevertheless be subject to relevant protective requirements, including safeguards against harmful dependency, privacy and security requirements, independent testing and

proportionate monitoring. The Regulation should expressly bring these systems within the scope of those requirements without subjecting them to the minimum-age restriction proposed for AI companions and general conversational chatbots.

Article 14 - Emotional dependency and independent testing

Article 14 addresses emotional dependency, testing and post-market monitoring, with an exemption from the specific post-market monitoring duty for micro and small enterprises.

It should identify more objective indicators of potentially harmful practices, including simulated exclusivity, guilt-inducing responses, pressure to return and discouragement of human relationships. Testing and monitoring should be subject to meaningful independent scrutiny. Ongoing research should inform assessments of emerging risks and potential benefits, including whether well-designed systems can support inclusion for children with disabilities or support needs.

The Regulation should address risks of dependency on AI systems beyond emotional dependency, including overreliance that may undermine children's independent thinking, learning and problem-solving skills. Age-appropriate prompts and pauses should encourage independent thinking, regular breaks and engagement in offline activities or learning outside the AI system. These measures should support children's agency and evolving capacities, while remaining accessible and accommodating children who use AI as an assistive tool.

When children use these systems for learning, providers should ensure that their systems prioritise explanations, guiding questions and opportunities for independent attempts rather than immediately supplying complete answers. When relevant, providers should offer age-appropriate routes to trusted human support. For medical or mental-health concerns, systems should explain their limitations and direct children to appropriate qualified professionals or confidential support services, without assuming that involving a parent or guardian is always safe or appropriate.

Article 15 - Minimum age for access to online games and time limits

Article 15 allows minors under 13 to access online games when guardian tools enable and control access. Still, unlike Article 7 for child-specific video-sharing services, it does not set a lower minimum age.

The Regulation should establish, at minimum, the same lower age threshold for online games as Article 7(4)(b) establishes for child-specific video-sharing services. Providers should not enable children under three to access online games. Higher minimum ages should apply where warranted by the game's content, features and risks. Article 15 should require child-specific online games to demonstrate they are age-appropriate before allowing access. Guardian involvement should be complementary to those protections. Codes of conduct can support implementation but must not create a presumption of compliance. The Regulation should require an evidence-based developmental approach to children's access to online games. Minimum ages, permitted features and protective measures should reflect

children's evolving capacities and the risks associated with each game's content, design, contact functions, monetisation and data practices.

Providers should demonstrate age-appropriateness through child-rights risk assessments and proportionate independent review before making a game available to children. Assessments should establish suitable age ranges and binding safeguards, including restrictions on particular features where necessary. Neither an age rating nor guardian authorisation should substitute for this assessment.

Access and basic protection should not depend on guardian availability or the activation of guardian tools. Providers should implement safeguards directly, with optional guardian involvement offering complementary support. Games or features whose risks cannot be adequately mitigated for a particular age group should remain unavailable to that group, regardless of guardian permission.

Children under 13 should have access only to games offering the highest level of protection, with strict safeguards built into their design. From age 13, children should be able to access age-appropriate games independently, with binding safety-by-design protections. Higher minimum ages should apply where justified by the risks. Providers should demonstrate age-appropriateness before allowing access. Guardian tools should offer optional additional support; access and basic protections should not depend on guardian availability or involvement.

Safeguards for children under 13 should include:

- Age-appropriate content and features, assessed before access is allowed.
- Private accounts by default, with geolocation and tracking disabled.
- No contact from strangers, public discoverability or automatic group additions.
- No behavioural advertising, paid loot boxes or manipulative spending prompts.
- No addictive design, with built-in time limits and regular breaks protecting sleep and school time.
- No AI companions or general conversational chatbots embedded in games.

Children aged 13-17 should have greater independent control, while retaining strong privacy, contact, spending and time-management protections. Providers should demonstrate suitability for the child's age and developmental stage before allowing access. Access and basic protections should not depend on guardian involvement.

Providers should enforce daily limits and regular breaks based on evidence about children's age, developmental needs, and the game's risks, including cumulative use and effects on sleep, education, and other activities. As an additional precautionary safeguard, a maximum cumulative ceiling of two hours per day should apply across online games for children aged 13-17, with shorter limits wherever the evidence warrants. The one-hour daily ceiling proposed above should apply to children under 13. Neither ceiling should be interpreted as a recommended or universally safe duration. Implementation should preserve privacy and accommodate narrowly defined, necessary assistive uses.

Articles 15, 18-21 - Equivalent protection in online games

Video games fall within the online-games category covered by Articles 18 and 20. Still, they are not expressly included in the provider categories listed in Articles 19 and 21.

The Regulation must expressly extend Article 19's child-friendly reporting and support obligations and Article 21's representation and complaint rights to individual video games. Even games without chat or multiplayer features may expose children to harmful content, intrusive data practices, pressure to spend or design features that undermine their safety. Children should have accessible ways to report these concerns and seek support and redress. Reporting should complement Article 18's feedback and control tools, which allow children to express preferences without alleging harm.

Articles 16 and 20 - Guardian tools for app stores

Article 16 sets out obligations for app stores regarding age-appropriate access to applications and refers to guardian tools under Article 20.

App stores should provide age-appropriate safeguards by default, independently of whether guardian tools are activated. These protections should cover browsing, downloading, and purchasing, including account-free access where available. Guardian tools should complement providers' binding obligations, rather than serve as a condition for children to benefit from protection or access age-appropriate applications. Their use should respect children's privacy and evolving capacities.

Article 18 - Accessibility and independent use

Article 18 requires child-facing features, information and user-control tools to be easily accessible to all minors and presented in a way they can understand.

The Regulation should strengthen this obligation by expressly requiring features, communications, warnings, information and user-control mechanisms to be accessible, understandable and usable by children of different ages. For children with disabilities, this should include compatibility with assistive technologies, alternative formats and navigation, and adaptations addressing cognitive and communication needs, such as simplified language. Children should be able to exercise these controls independently wherever appropriate, taking account of their evolving capacities, with support available when needed.

Information, reporting tools, support, and content moderation should accommodate children's diverse linguistic and communication needs, including languages beyond national official languages and accessible formats such as Braille, sign languages, and easy-to-read information, so all children can access protection, participate, and obtain help and redress.

Article 18 - Controls to disable short-form video feeds and sequential ephemeral-content features

Article 18 requires providers to offer accessible tools that let children control the content and recommendations they encounter, with immediate and durable effects.

The Regulation should require short-form video feeds and sequential ephemeral-content features, such as Shorts, Reels and Stories, to be disabled by default and unavailable for activation for children under 15. For older children, providers should offer a prominent, accessible and easy-to-use option to disable them. This means removing their dedicated entry points, previews, recommendations, and related notifications throughout the service, without restricting access to other functionality. The choice should take effect immediately, remain in place across sessions and devices, and be usable independently of guardian involvement. Providers should not automatically reactivate these features or use repeated prompts or incentives to encourage reactivation. This should complement Article 9's safeguards against design that encourages compulsive or excessive use.

Article 19 - Child-friendly reporting

Article 19 requires accessible reporting, priority handling without undue delay, information about the procedure undertaken and available possibilities of redress, and access to support and authoritative information.

It should specify the additional safeguards needed for reporting to work in practice, including accessibility for children with disabilities, clear routes to trusted human support where appropriate, and processes that children of different ages can understand, use and follow. Where the Regulation establishes expert work, codes, monitoring or later technical rules, their terms of reference should require child-friendly participation. Child-friendly reporting mechanisms should explicitly include disability-accessible reporting.

Article 20: Guardian tools

Article 20 requires providers of social networking services, video-sharing platforms, online games, AI companions, and general conversational chatbots to provide effective, accessible, and user-friendly guardian tools. These tools must reflect children's age and gradual development, respect their agency and privacy, and avoid disproportionate restrictions on their rights.

Guardian tools should accommodate diverse family structures, care arrangements and shared parental responsibility, allowing multiple authorised carers to provide support without conflicting controls or disruption to the child's account. The Regulation should clarify how these tools work when guardianship changes, when children or their families are in different care and migration circumstances.

Their design should also accommodate legally authorised professionals supporting several children, within their lawful mandates. Building on Article 31(2)-(3), the Regulation should require workable, accessible procedures for children in alternative care, refugee and displaced families, and unaccompanied children. Implementation arrangements should take into account that Article 23(10) of the Asylum Procedures Regulation normally limits a

representative's responsibility to 30 unaccompanied children simultaneously, rising to a maximum of 50 in exceptional circumstances.

These procedures should accommodate authorised professionals supporting several children, changes in care arrangements, and shared parental responsibility, including where parents are separated or divorced. Recital 59's principle of non-exclusion should be made explicit in the operative provisions: no child should lose the Regulation's protections because of their family's administrative, social or residence situation.

Specific safeguards are needed where children experience domestic violence or abuse. The Regulation should clarify when an adult's access to guardian tools must be restricted or withdrawn, consistently with applicable law and protective decisions, to prevent those tools from enabling coercive control or further harm.

These arrangements should also cover situations where no guardian is available or can safely support the child, where parental responsibility is disputed or subject to legal restrictions, and where care or guardianship changes across borders. Providers should establish clear procedures for granting, transferring, suspending, and withdrawing access to guardian tools; verifying each adult's lawful authority; and resolving conflicting instructions without disrupting the child's account, legitimate contacts, or confidential support. Children should have accessible ways to challenge incorrect or abusive use of these tools and obtain timely human review.

Guardian tools should respect children's privacy, agency, and evolving capacities; avoid disproportionate monitoring of communications, searches, or online activity; and preserve confidential access to trusted support and helplines. Adult support should complement providers' responsibility to make services safe by design, and children's basic protections should not depend on a guardian's availability or capacity to use these tools.

These requirements should extend to reporting channels, complaints and redress mechanisms, age-assurance processes and support tools under the relevant provisions. Providers should systematically involve children with different disabilities in testing these safeguards and demonstrate that they can understand and use them in practice.

Accessibility should also address barriers associated with poverty, migration, care arrangements, low literacy or digital skills, and limited access to adult guidance. Providers should assess how these circumstances affect children's ability to use safeguards, adopting a gender-sensitive, intersectional approach so protections work across social contexts.

Interoperability should allow guardians to use compatible tools across services without creating a central record of children's activity or enabling cross-service tracking. Common standards should preserve service-specific safeguards and children's privacy.

Article 22 - Monitoring the effectiveness of safeguards

Article 22 requires providers of services referred to in Article 8(1) that are designated as very large online platforms to monitor, test and evaluate the effectiveness of their Chapter III measures. This evaluation must form part of their risk assessment under Article 34 of the DSA. Article 14 separately requires post-market monitoring for AI companions and general

conversational chatbots, while exempting micro and small enterprises from that specific duty.

Proportionate monitoring, testing and evaluation should extend to AI companions, general conversational chatbots and online games beyond those covered by Article 22, according to their risks to children. Providers should demonstrate that safeguards remain effective, assess differential and cumulative impacts on children's rights, and take corrective action in response to emerging harms. Smaller providers should receive practical support to meet these obligations, without leaving significant risks unmonitored.

Articles 22, 25, 37 and 42 - Continuous research and adaptation

The proposal provides for monitoring the effectiveness of safeguards under Article 22, updating specified safety measures under Article 25, developing supervisory expertise and capabilities under Article 37, and reviewing the Regulation under Article 42.

These mechanisms should be informed by continuous, independent research into evolving design practices, AI companions and conversational chatbots, gaming monetisation, accessibility, and the real-world effects of age restrictions on different groups of children. Research should examine emerging harms, potential benefits and unintended consequences, with particular attention to children in vulnerable situations. Findings should inform guidance, enforcement, updates to safety measures and the review of the Regulation.

Article 26 - Privacy-preserving verification of parental responsibility

Article 26 concerns verification of parental responsibility when creating limited accounts under Article 6(2), enabling guardian-controlled access to child-specific video-sharing services under Article 7, and implementing guardian tools under Article 20(1). It permits providers to use signals from official databases or interfaces and requires verification to be privacy-preserving.

The Regulation should ensure that all official signals and interfaces used under Article 26 to verify parental responsibility give practical effect to this safeguard, without exposing underlying family records. Before requiring or recommending a particular method, the Commission should assess feasibility, enforceability, cost, accuracy, accessibility and data-protection impacts across national systems. Verification procedures should accommodate lawful care arrangements and provide accessible alternatives where standard civil-status documentation is unavailable. If verification relies on official databases, Member States should assess whether suitable records exist, remain current, and can be lawfully accessed through interoperable systems.

Article 26 - Avoiding self-declaration as proof of parental responsibility

Article 26 permits providers to accept an adult's self-declaration of parental responsibility when creating limited accounts under Article 6(2), enabling guardian-controlled access under Article 7, or implementing guardian tools under Article 20(1), at least until the delegated act referred to in the provision is adopted. Providers must nevertheless make reasonable efforts to verify that the adult exercises parental responsibility.

The Regulation should require reliable, proportionate, privacy-preserving verification when an adult activates guardian tools or exercises functions reserved to a holder of parental responsibility; self-declaration alone should not suffice. Accessible alternatives should ensure that children are not excluded when an official interface is unavailable. In line with the amendments proposed to Article 6, verification of parental responsibility should not be a prerequisite for children aged 13-14 to create or continue using a limited account independently of guardian tools. Verification should remain required for guardian-held accounts under Article 7 and when adults activate guardian tools.

Articles 27-31 - Age assurance

Articles 27-31 require accurate, reliable, secure, robust, non-intrusive, privacy-preserving and non-discriminatory age assurance. Article 28 requires state-of-the-art technology and zero-knowledge proofs, limits personal-data processing to what is strictly necessary, and prohibits identification, location, tracking, targeting, advertising, profiling and further processing, sharing or combining age-assurance data, subject to specified exceptions for minimal age-signal retention and consent-based sharing through operating systems. Articles 29-30 establish certified third-party EU age-verification solutions for Article 6, conditions for alternative age-assurance methods, free procedures for challenging incorrect outcomes, and technical requirements. Article 31 requires Member States to provide free, accessible means of proving parental responsibility without disclosing underlying records, alternative procedures where standard documentation is unavailable, and at least one free certified EU age-verification solution for citizens and residents.

Age assurance should establish only whether a user meets the relevant age threshold or falls within the necessary age range. It should be separated from the platform and handled by independently assessed third-party services. Personal data should be processed solely to establish the necessary age attribute, with no advertising, profiling, model training or other secondary use. Sensitive input data should be deleted once the assessment is complete. Proof presentation should disclose only the necessary age threshold or range, prevent cross-service tracking, and ensure that the assessment provider does not learn where proofs are used. The technical rules under Article 30 should distinguish the processing necessary to establish an age attribute from the subsequent presentation of proof to a service. A publicly accessible list should identify independently assessed providers and solutions that meet the applicable certified standards, with transparent criteria, ongoing oversight, and procedures for suspension or withdrawal when compliance fails. Inclusion should not remove service providers' responsibility to ensure that their chosen method is appropriate to the relevant age, risk and accessibility needs.

The EU should continue improving and independently assessing its age-verification app and supporting infrastructure, with particular attention to security, privacy, reliability, accessibility and usability. The EU should fix identified vulnerabilities, retest them, and keep safeguards under ongoing scrutiny. Alongside this work, the EU should fund shared, independently assessed infrastructure and services for age assurance, including age estimation, building on its existing blueprint and supporting other suitable methods where

necessary. Smaller providers should be able to access, integrate and use these services free of charge or at affordable cost.

Independent assessment should test accuracy, privacy, security, accessibility and resistance to circumvention under real-world conditions. Testing should examine both children incorrectly classified as older and users wrongly denied access, with results broken down by relevant age groups and assessed for discriminatory outcomes. It should also address shared devices, multiple users and changes of user, so that an adult's age signal does not automatically authorise a child's access. Measures to prevent circumvention should not introduce disproportionate identification, tracking or data retention.

Funding should support the organisations developing and providing these services, rather than direct financial transfers to platforms. It should cover development, maintenance, operation, independent assessment, continuing security testing and technical support for integration. Larger platforms should bear their own implementation and operating costs and could contribute to maintaining the shared infrastructure.

This investment should strengthen European technological independence through open, interoperable infrastructure under effective EU governance and supervision. Procurement should ensure strong safeguards across providers and subcontractors, minimise personal data processing, prevent tracking across services and avoid dependence on a single supplier. Solutions should be accessible, non-discriminatory and appropriate to the ages, services and risks concerned.

Technical standards, assessment criteria and meaningful summaries of independent testing should be publicly available. Open-source components should be supported to enable scrutiny, alongside independent examination of deployed systems and their data flows. Certification should include ongoing oversight, reassessment following material changes, and procedures for addressing vulnerabilities and suspending non-compliant solutions. Commercial confidentiality should not prevent regulators and authorised independent assessors from examining compliance.

Users should receive accessible, age-appropriate explanations of age-assurance decisions and have free, timely ways to challenge incorrect outcomes, including human review where necessary. Alternative compliant methods should be available where a user cannot use the initial method because of disability, lack of documentation, technical barriers or an incorrect result. Correcting an error should not require unnecessary disclosure of identity or family information. Children should be able to challenge an incorrect outcome without mandatory guardian involvement, while access to age-restricted services remains subject to the applicable safeguards. Providers should document and independently evaluate the reliability of any evidence used to waive an age check, including whether it relates to the current user rather than another person using the same account or device.

Article 32 - Reliable evidence for age-assurance exceptions

Article 32 allows providers to forgo certain age checks where they can establish, with a high degree of confidence, that a user has reached the relevant minimum age or is an adult.

The Regulation should clarify which evidence providers may rely on and how its reliability must be demonstrated, including the risk of wrongly classifying children as adults. For instance, a previously used payment method should not automatically establish the current user's adulthood.

Article 33 - National strategies, inequality and civil society

Article 33 concerns Member State measures to prepare and support minors.

National strategies should explicitly address the digital divide, recognising that meaningful access requires more than connectivity. Measures should ensure affordable, reliable internet, suitable devices and assistive technologies, accessible services, digital skills, trusted support and effective routes to help and redress. Strategies should be linked to the European Child Guarantee and prioritise children in vulnerable situations, including children experiencing poverty or housing deprivation, children with disabilities, migrant and refugee children, children from minority ethnic backgrounds, children in alternative care and children in precarious family situations.

Digital and media literacy education should go beyond technical skills and avoiding online risks. It should help children understand and exercise their rights, critically assess information, protect their privacy and personal data, and recognise how service design, recommender systems, advertising, and manipulative or addictive features can influence their choices. Children should learn how to use safety and reporting tools, seek trusted support and obtain redress.

Strategies should provide sustained, accessible, age-appropriate learning in schools and community settings, with targeted support to overcome language, disability, financial, and other barriers. Parents and caregivers, teachers, and educators should receive practical guidance and training tailored to their roles, along with opportunities to learn with children and discuss their digital experiences. These measures should support children's gradual transition to safe and autonomous online use without shifting providers' safety responsibilities onto children or families.

National strategies should also ensure access to independent, regularly updated information services for children, parents and other caregivers. Building on Safer Internet Centres and trusted civil-society organisations, these services should explain the purpose, uses and key features of platforms children use, including their safety settings, contact functions, recommender systems and commercial practices. Information should be accessible, child-friendly and free from commercial influence, supporting informed choices and conversations about children's digital experiences. This support should complement binding provider obligations and guardian tools.

Civil-society organisations, including those working with children in vulnerable situations, should be supported alongside Safer Internet Centres. Children should participate meaningfully in developing and evaluating these strategies, and these strategies should also improve access to affordable, inclusive offline activities.

Article 40 - Independent expertise

Article 40 establishes a Child Safety Committee to assist the Commission.

The Committee's work should be systematically informed by independent research, child-rights and disability expertise, relevant experts from the Special Panel on Child Safety Online, and children's perspectives. The Regulation should establish clear arrangements to obtain this input through advisory or consultative roles compatible with the Committee's formal structure.

Article 42 - Review of interaction with other EU law

Article 42 provides for a review of the Regulation.

That review should explicitly examine how it works alongside the DSA, AI Act, GDPR and AVMSD, and, if adopted, EU legislation on digital fairness. It should identify overlaps, gaps and inconsistencies in duties, supervision and enforcement. Building on Article 34(7), the Regulation should clarify practical arrangements for cooperation and coordination between the authorities responsible for implementation and enforcement.

The review should assess whether the Regulation effectively protects children using educational AI, including specialised conversational systems and AI embedded in educational services. It should examine the interaction between the educational exemption in Article 2, the definitions in Article 3 and the protective obligations in Article 14 and related provisions. Where gaps remain, the Commission should propose legislative amendments to ensure effective protection while preserving the targeted exemption from age-based access restrictions.

Embedding children's participation

The proposal establishes a Child Safety Committee under Article 40 and recognises children's contributions to the consultations informing the Act.

Children and adolescents should be systematically involved in the development, testing, monitoring and review of measures adopted under the Regulation. Participation should be meaningful, inclusive and adapted to age and evolving capacities. Member States should meaningfully involve children before implementation and in evaluating which measures work in practice and what changes are needed. Member States should publish annual implementation evaluations, informed by children's views and independent research. These should examine effects on children's rights, safety, well-being and inclusion, including movement to higher-risk services and the effectiveness of provider safeguards and guardian tools.

Children should also participate in developing and reviewing child-friendly community standards and content-moderation policies, helping providers understand what content and behaviour they experience as harmful and whether moderation, reporting and appeal processes work for them. Participation should be inclusive and safeguarded, without exposing children to harmful material or shifting providers' responsibilities onto them.

Accessibility by design

The proposal considers children with disabilities: recital 41 explicitly recognises their accessibility needs, Article 18 requires child-facing features and tools to be accessible and understandable to all minors, and Article 31(2) expressly addresses accessibility for persons with disabilities when verifying parental responsibility.

The Regulation should explicitly require providers within its scope to design and test safety features, privacy settings, reporting mechanisms, recommender controls, age-assurance processes and guardian tools in accordance with the principles of universal design and accessibility by design. This should include compatibility with relevant assistive technologies and accessible alternatives, such as screen readers, alternative input devices, captions, text-to-speech, speech-to-text and simplified interfaces.

Particular attention should be paid to children with intellectual disabilities, autistic children and children with communication, cognitive or sensory disabilities. Accessibility should address comprehension, communication and independent use, alongside technical compatibility. Providers should involve children with different disabilities in testing these safeguards and demonstrate that they can understand and use them in practice.

These requirements should complement, and be without prejudice to, obligations under the European Accessibility Act where applicable. Protective features, including age-verification interfaces, guardian dashboards, reporting mechanisms and controls, should be accessible to children, parents and carers with disabilities. This should include compatibility with assistive technologies, understandable information and accessible alternatives addressing sensory, physical, cognitive and communication needs. Providers should involve parents and carers with different disabilities in testing these tools. No child should lose access or protection because an authorised adult cannot use an inaccessible verification process or guardian tool.

For more information, contact:

Francesca Pisanu
Senior Policy Officer, Eurochild
francesca.pisanu@eurochild.org

Eurochild AISBL

Avenue des Arts 7/8, 1210 Brussels
Tel. +32 (0)2 511 70 83
info@eurochild.org – www.eurochild.org

© Eurochild 2026