KOYUNCUOĞLU & KÖKSAL

SUMMARY BRIEFING ON APPROACHES TO CHILDREN'S ONLINE SAFETY AND TÜRKİYE'S NEW REGULATION ON SOCIAL NETWORK PROVIDERS

1. INTRODUCTION

The Regulation on the Provision of Age-Segregated Services for Children and Age Verification by Social Media Providers (No. 33396), published in the Official Gazette on October 10, 2026 ("Regulation"); was issued to establish the procedures and principles regarding age verification for access to services provided by social media providers, the provision of age-appropriate, segregated services for children, and parental control tools. In accordance with the Regulation, its primary objective is to ensure the enforcement of age restrictions on children's access to social media services and to guarantee that children are in a safe digital environment appropriate for their age and maturity level.

The protection of children in the online environment is an area of regulation that has become increasingly important worldwide with the advancement of digital technologies. While new regulations in this area are being implemented in Turkey, various legal regulations and guidelines aimed at protecting children's online safety and privacy are also being published at the international level. These developments demonstrate that the protection of children in the digital environment has become one of the primary issues on a global scale.

2. AGE VERTIFICATION VE PARENTAL CONTROL TOOLS

2.1. Age Verification Obligation and Fundamental Principles

In accordance with Article 5 of the Regulation, all social media providers—whether based domestically or foreign—are required to implement age verification mechanisms to prevent children under the age of 15 from accessing social media and to ensure a safe environment for children between the ages of 15-18. Article 6 of the Regulation requires all social media providers to take the necessary technical and administrative measures to ensure compliance with these obligations. Accordingly, users' ages must be verified using an age verification token during the account creation process.

The regulation stipulates that social media providers must use an age verification token which is a*technical verification tool that indicates the user's age threshold* [1] for age verification; it further stipulates that this token must be technically reliable, consistent, auditable and testable. It also

[1] https://www.resmigazete.gov.tr/eskiler/2026/10/20261010-15.pdf art.4 (f)

specifies that age verification methods and parental control tools must be designed in a way that does not cause discriminatory outcomes and is accessible to all users, including individuals with disabilities.

In addition, pursuant to Article 7 of the Regulation, age verification during the account creation process upon request may be conducted through the e-Government Portal via the online service provided by the Cybersecurity Presidency, by uploading the "age verification token" generated through this process to the relevant social media platform. Social media providers determine the user's age group based on the age verification token generated by the Presidency and may not use the age verification token for any purpose other than age verification.

Furthermore, following the primary age verification, social media providers may also implement single-step or multi-step age verification methods of their own choosing for the duration of the service. However, these methods must comply with the principles specified in the Regulation regarding reliability, algorithmic transparency, the prohibition of discrimination, and the protection of personal data. In this context, methods that allow only for determining whether the relevant age threshold has been met—rather than direct identity verification—should be used, and personal data should not be processed for purposes other than age verification. The age verification token must contain information indicating whether the user has reached the age of 15 and, if so, whether the user has reached the age of 18; it must not contain any personal data other than this information, such as a username or any other information that could identify or make the individual identifiable, and it must be used only for the purpose of age verification.

The purpose of this system is for the social media provider to verify only whether the relevant age threshold has been met, rather than obtaining the user's identity or date of birth. In this way, the process of age verification is separated from the social media provider's collection of the user's identity information.

On July 14, 2025, the European Commission published a prototype application and a technical framework for online age verification.[2] This approach aims to enable users to prove that they meet a certain age threshold without unnecessarily disclosing their exact age or identity. In addition, the Commission has agreed on a recommendation that will pave the way for universal access to anonymous age verification tools that ensure the highest possible standards of privacy and data protection; By using "*Zero-Knowledge Proof (ZKP)*" encryption, the goal is to prevent third parties

[2] https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification

from tracking which content users access and to ensure that the age verification process is not linked to users' identities or their online activities. The Commission has proposed the creation of an EU Age Verification Scheme to identify reliable age verification providers and age verification solutions.

In the United Kingdom, under the *Online Safety Act 2023*, the age verification guidance published by Ofcom focuses on ensuring that the methods used to prevent children from accessing harmful content meet the standard of "*highly effective age assurance*" in relation to the proposed restriction on social media use by children under the age of 16.[3] According to Ofcom's guidance, methods considered highly effective include open banking, photo ID matching, facial age estimation, mobile network operator age checks, credit card checks, digital identity services and email-based age estimation. By contrast, self-declaration of age by users and online payment methods that do not require users to be at least 18 years old are not considered effective methods.

While Türkiye's approach to the creation and use of the age token is based on a verification mechanism provided by the public authority through the Regulation, the e-Government Gateway and the Presidency, the European Union envisages a solution based on common technical standards. This solution may be integrated into national digital identity wallets by Member States or offered as a standalone application. It also enables private-sector actors to develop solutions in accordance with this technical framework and aims to ensure adaptability across different services.

Nevertheless, both approaches share the common objectives of ensuring that age verification is carried out reliably, avoiding the unnecessary disclosure of personal data and safeguarding users' privacy.

2.1. Parental Control Tools

In the Regulation, parental control tools are defined as *technical tools that allow the management of content, access, screen time, purchasing, and privacy settings, as well as the monitoring of usage activities, in order to protect children from the risks of age-inappropriate content, harmful online interaction, and excessive use*, and technical tools that provide the management of platform settings and the monitoring of usage activities.[4] These are technical tools that enable the management of platform settings and the monitoring of usage activities. Pursuant to the Regulation, social network providers are required to offer parental control tools that are clear, understandable and user-friendly. It is specifically emphasized that the provision of such tools does not exempt providers from their

[3] https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-to-protect-children-online
[4] https://www.resmigazete.gov.tr/eskiler/2026/10/20261010-15.pdf art.4 (d)

obligation to offer differentiated services specifically designed for children who have reached the age of 15.

The Regulation provides that parental control tools are to be used by persons having parental authority or decision-making responsibility over the child, such as parents or legal guardians, and stipulates that these tools must include, at a minimum, the following functionalities:

- Control over account and feature settings,
- Subjecting purchases, rentals and paid subscription transactions to parental permission or approval, and setting spending limits for such transactions,
- Monitoring, determining and restricting usage time by parents,
- Providing control mechanisms regarding location sharing.

The Regulation stipulates that the parental control tools to be provided must include a Turkish language option, be easily accessible and activatable, function across different devices and operating systems, and clearly notify the child when they are activated. It also requires the adoption of measures to prevent the parental control authority, or any changes made to such authority, from being disabled or removed by the child without the parent's knowledge. Furthermore, the Regulation requires that parental control should not disproportionately undermine the child's privacy and should be based on communication, learning and empowerment rather than surveillance. Consequently, parental control is viewed not as an unlimited monitoring authority, but as a tool that requires striking a balance between the child's safety and privacy.

The European Commission's DSA Guidelines[5], recommend the provision of software that helps parents support their children's online activities, privacy, safety and well-being, while respecting children's autonomy and privacy. In this regard, functionalities such as the management of account settings, the limitation of screen time and the management of online interactions are particularly emphasized. The Regulation, on the other hand, sets out the minimum functionalities of parental control tools in more specific terms, requiring, inter alia, control over account and feature settings, subjecting purchases and rentals to parental approval, setting spending limits, monitoring and restricting usage time and providing mechanisms for controlling location sharing.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025XC05519 art.7.3 "*Tools for guardians*"

The European Commission's Guidelines emphasize that parental control tools should support communication, learning and empowerment, in addition to monitoring and restriction, and should not disproportionately interfere with children's rights to privacy and autonomy. The Regulation likewise stipulates that parental control should be designed in a manner that safeguards children's privacy and supports their development.

While both approaches aim to strike a balance between the protection of children and their rights and freedoms, the Regulation provides for a more detailed framework regarding the minimum functionalities and technical requirements of parental control tools.

3. DIFFERENTIATED SERVICES DESIGNED SPECIFICALLY FOR CHILDREN

Pursuant to the Regulation, while account creation requests submitted by individuals identified as being under the age of 15 following age verification are rejected, the accounts of children who have reached the age of 15 are subject to the principles governing differentiated services set out in Article 8 of the Regulation. Differentiated services are defined *as social network services provided by social network providers to children who have reached the age of 15, incorporating safety, privacy, content presentation, algorithmic, communication and parental control features appropriate to their age and level of development.*

Under the envisaged service model, social network providers are required to take into account the child's age, best interests and the protection of their physical, psychological and emotional development, as well as the prevention of risks of sexual abuse and commercial exploitation, when designing content, advertising and other services intended for children who have reached the age of 15. Furthermore, in order to protect children's personal data, high levels of privacy settings must be applied by default, data processing must be limited to the minimum necessary, and contracts, user settings and data policies must be presented in a manner that children can understand. In this respect, differentiated services encompass not merely the creation of a separate account based on age, but also content presentation, communication between users, recommendation algorithms and the processing of personal data.

The provision of services that may lead to addictive behavior is prohibited in children's accounts. The Regulation further stipulates that such accounts must be private by default, that information regarding followers and followed accounts must be concealed, that messaging must be restricted to accounts followed by the child, and that the synchronization of contact lists and the recommendation of children's accounts to one another must be prevented. In addition, the Regulation provides for the

prevention of screenshots and live streaming, the restriction of consecutive visual content feeds, and limitations on behavioral personalization and personalized commercial advertising.

The European Commission's DSA Guidelines[6], DSA Guidelines recommend that children's accounts be private by default, that recommender systems be configured to reduce the risk of children being exposed to harmful content, and that children be given greater control over their content feeds. The Guidelines also address measures to mitigate the risk of children's content being downloaded or screenshotted by others, as well as measures such as disabling by default features that encourage excessive use, including autoplay, communication streaks and read receipts. In this respect, the European Union's approach pursues a protective objective similar to that of the Regulation in Türkiye.

In Australia, following an amendment to the Online Safety (Age-Restricted Social Media Platforms) Rules 2025, made pursuant to the Online Safety Act 2021, design features such as infinite scrolling, feedback mechanisms including like and upvote counts, and time-limited content such as disappearing stories were added to the design elements taken into consideration when determining whether social media platforms fall within the scope of age restrictions.[7] Under the Australian approach, the protection of children takes into account not only the nature of the content but also the design features of platforms that are intended to increase user engagement and the amount of time spent on screen.[8]

4. APPLICATION AND APPEAL MECHANISM

Pursuant to Article 10 of the Regulation, social network providers are required to establish an application and appeal mechanism in Turkish that is free of charge and accessible, in order to ensure the prompt resolution of appeals concerning age verification results, the suspension or termination of accounts, and measures implemented within the scope of differentiated services. Applications may not be assessed solely through automated systems and must be subject to meaningful human review. The content and personal data associated with an account may not be deleted until the application has been resolved. Notifications of decisions must inform users of their right to lodge a complaint with the Presidency and to seek judicial remedies. Furthermore, data concerning the number of applications and appeals, acceptance rates and average resolution times must be reported to the Presidency annually and published on the providers' websites. Through this framework, the Regulation ensures that users have access to application and appeal procedures in cases where age verification systems

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025XC05519 art.6.3.1 & art. 6.5
[7] https://www.legislation.gov.au/F2025L00889/2026-03-26/2026-03-26/text/original/epub/OEBPS/document_1/document_1.html art.4(A)
[8] https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions

produce erroneous results or measures imposed on children's accounts are found to be erroneous or unlawful.

The European Commission's DSA Guidelines[9], recommend the provision of easily accessible reporting tools, prompt feedback on reports, and the development of internal complaint-handling mechanisms in order to enhance children's online safety. The Regulation in Türkiye adopts a similar approach by requiring social network providers to establish an application and appeal mechanism concerning age verification results and certain measures imposed on accounts.

5. SANCTIONS AND COMPLIANCE PROCESS

Pursuant to the Regulation, accounts created before its effective date and not verified through an age verification token must be verified at least once by 31 March 2027. Following verification, accounts belonging to children identified as being under the age of 15 must be closed upon notification to the user, while accounts belonging to children who have reached the age of 15 must be subject to the principles governing differentiated services.

Article 11 of the Regulation provides that sanctions shall be imposed in the event of non-compliance with the specified obligations, and that the relevant provisions of Additional Article 4 of Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications ("Law No. 5651") shall apply with regard to the notification of sanctions, appeal procedures and their removal. Accordingly, the Regulation does not establish an independent sanctions regime, but rather refers to the existing statutory framework.

Pursuant to Additional Article 4 of Law No. 5651, where social network providers fail to fulfil their obligations concerning the protection of children[10];

- An administrative fine of up to 3% of their global turnover in the preceding calendar year may be imposed,
- If the non-compliance continues, an advertising ban may be imposed.
- Subsequently, pursuant to a decision of the Criminal Judgeship of Peace, internet traffic bandwidth may be throttled by up to 50% and, at a later stage, by up to 90%.

Before any sanction is imposed, the social network provider must be notified of the non-compliance and granted a reasonable period of time to remedy it. In determining the applicable sanction,

[9] https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors
[10] https://www.lexpera.com.tr/mevzuat/kanunlar/internet-ortaminda-yapilan-yayinlarin-duzenlenmesi-ve-bu-yayinlar-yoluyla-islenen-suclarla-mucadele# additional art.4 (24)

consideration shall be given to the severity and duration of the non-compliance, the number of children affected, and the provider's good-faith efforts to achieve compliance.

Article 12 of the Regulation authorizes the Cybersecurity Presidency to prepare guidelines on the technical structure of the age verification token, the format of the information it contains, and the verification process, as well as to determine the procedures and principles governing the implementation of the Regulation.

Nevertheless, it may be argued that the Regulation has certain aspects that require further development in terms of sanctions and institutional structure. Although significant responsibilities are assigned to the Cybersecurity Presidency in the implementation of the Regulation, the protection of children in the online environment is not limited solely to technical age verification systems and the obligations of social network providers. The development of children's digital literacy, raising parental awareness, protecting children's personal data, and reducing online risks through education are also integral components of a comprehensive child protection approach. Therefore, clearly defining the roles and responsibilities of institutions such as the Ministry of National Education, the Ministry of Family and Social Services, and the Personal Data Protection Authority within the framework of the relevant legislation, as well as establishing inter-institutional cooperation and coordination mechanisms, is important for the effective implementation of the Regulation.

International examples demonstrate that the online protection of children can be supported through the involvement of different institutions. In Ireland, Coimisiún na Meán not only oversees platforms' compliance with their online safety obligations but also provides information and digital media literacy resources for children, parents and teachers.[11] Accordingly, ensuring the effectiveness of the Regulation requires consideration not only of the imposition of sanctions on platforms, but also of clarifying the responsibilities of relevant public institutions, ensuring inter-institutional coordination, and supporting awareness-raising initiatives targeting families and educational institutions.

In addition, the protection of children's personal data also falls within the jurisdiction of independent data protection authorities. For example, in the United Kingdom, pursuant to Section 123 of the Data Protection Act 2018,[12] the data protection authority, the ICO, has been tasked with developing a code of practice regarding the age-appropriate design of online services that children are likely to access. Thus, the online protection of children falls within the statutory remit of the data protection authority

[11] https://www.cnam.ie/general-public/guides-resources/
[12] https://www.legislation.gov.uk/ukpga/2018/12/section/123

not only in terms of platform safety and content moderation, but also with regard to the protection of children's personal data and the privacy-oriented design of services. This highlights the importance of data protection authorities playing an active role, within the scope of their respective powers, in regulatory frameworks aimed at protecting children online.

In this regard, in addition to the role of the Cybersecurity Presidency in the implementation of the Regulation in Türkiye, explicitly establishing a coordination mechanism consistent with the existing powers of the Personal Data Protection Authority in matters concerning the processing of personal data during age verification, data minimization and the protection of children's privacy, while also involving other relevant institutions, such as the Ministry of National Education, could contribute to a comprehensive approach to the protection of children.

6. CONCLUSION

The Regulation published in the Official Gazette (Regulation on the Provision of Differentiated Services Specifically Designed for Children and Age Verification by Social Network Providers) establishes a legal framework aimed at ensuring that children are protected in the digital environment and provided with a safe online environment appropriate to their age and level of development. Within this framework, the age verification token mechanism, implemented through the cooperation of the e-Government Gateway and the Cybersecurity Presidency, prioritizes user privacy by preventing platforms from directly collecting identity or date-of-birth data and focusing instead on verifying whether the relevant age threshold has been met. At the same time, strict safety measures are introduced for children who have reached the age of 15 but have not yet turned 18, including private accounts by default, restricted communication and recommendation algorithms, and measures to prevent addictive design practices. Parents are also provided with the means to manage account settings, subject purchases to parental approval, set spending limits and restrict screen time. However, these tools are expected not to disproportionately undermine children's privacy and to be based on empowerment.

Nevertheless, we believe that the full effectiveness of the Regulation does not depend solely on the technical compliance efforts of social network providers. In addition to the role of the Cybersecurity Presidency, the establishment of a comprehensive ecosystem involving relevant institutions such as the Ministry of National Education, the Ministry of Family and Social Services, and the Personal Data Protection Authority, together with efforts to enhance digital literacy and ensure inter-institutional coordination, will be of considerable importance.

The provisions introduced under the Regulation will enter into force on 1 November 2026, and existing accounts must be verified through the age verification token no later than 31 March 2027. Social network providers and relevant stakeholders must take this compliance timeline into account and promptly complete the necessary technical and administrative infrastructure preparations.

Kind Regards,

Koyuncuoğlu & Köksal Avukatlık Bürosu

**The explanations provided in this study have been prepared on the basis of the legislation currently in force in the Republic of Türkiye and the information made publicly available by the relevant official authorities. In respect of any matters of uncertainty, we recommend that you seek our advice and assistance before taking any final action. Otherwise, our Law Firm shall not be held liable for any actions taken on the basis of the explanations set forth herein or for the consequences thereof.*