Children's Data Security: Current Developments Worldwide and in Türkiye

In the digital ecosystem, children are no longer viewed solely as individuals in need of protection; they have also become one of the central user segments within data-driven business models. Social media platforms, gaming applications, and video-sharing websites systematically process children's behavioral data, interaction patterns, and content consumption habits. This reality has led to a transformation in the legal approach to children's data protection, shifting from a traditional consent-based model toward a risk-based regulatory framework.

At the present stage, the debate is no longer limited to the question of whether children's data may be collected. The core issues now concern whether profiling directed at children should be prohibited altogether; which age verification techniques can be considered legally legitimate, proportionate, and effective; whether platform design itself should become a direct subject of data protection scrutiny; and whether a "self-declared age" method based solely on user statements can be regarded as sufficient. In other words, regulators have moved beyond the traditional consent-centered framework toward a structural assessment that places children's rights at the center - at the level of design, algorithms, and business models. Recent global developments further confirm this transformation.

Global Developments in the Protection of Children's Data Privacy

United Kingdom – Information Commissioner's Office (ICO)

Recently, the United Kingdom's data protection authority, the Information Commissioner's Office ("ICO"), imposed a fine of £14.47 million on Reddit on the grounds that it had failed to process children's personal data lawfully. In its investigation, the ICO found that Reddit had not implemented an appropriate and effective age verification mechanism and therefore lacked a valid legal basis for processing the personal data of children under the age of 13. It was also determined that Reddit had failed to carry out a data protection impact assessment (DPIA) aimed at identifying and mitigating risks specifically affecting children. Due to these shortcomings, the ICO concluded that Reddit had unlawfully processed children's data and exposed them to the risk of encountering inappropriate and harmful content. Although Reddit introduced certain measures in July 2025—such as age verification for access to mature content and requiring users to declare their age when creating an account—the ICO emphasized that relying solely on user self-declaration is insufficient, as it is easily circumvented and poses inherent risks for child users.

China – Cyberspace Administration of China (CAC)

On 29 December 2025, through an announcement published by the China Data Protection Authority ("CAC"), an additional implementation measure to the Measures on the Protection of Minors in Cyberspace was introduced, imposing an annual reporting obligation on all data controllers processing the personal data of individuals under the age of 14. No exceptions have been предусмотрed, and all data controllers processing minors' personal data in any capacity are subject to this new reporting requirement.

In fact, data controllers in China were already under an obligation to conduct annual audits of their processing activities relating to minors' personal data. With the new regulation, this obligation has been expanded, making it mandatory to formally notify the CAC of a summary of the audit results. In addition to general data protection requirements, the Chinese data protection authority has stated that, with respect to children, audits must examine issues such as the preparation of privacy notices specifically tailored to children, age verification methods, parental consent mechanisms, and the establishment of policies and procedures specific to children's data.

U.S. Federal Trade Commission – FTC

The Federal Trade Commission ("FTC") has published a policy statement regarding its enforcement activities under the Children's Online Privacy Protection Act ("COPPA"). In its policy statement, the FTC positions age verification technologies as a critical tool for online child safety and encourages operators to adopt such technologies. The Commission announced that, with respect to general-audience or mixed-audience services that process data solely for the purpose of determining a user's age, it would take a non-enforcement approach under COPPA, provided that certain safeguards are met. These safeguards include: using the data exclusively for age determination purposes; avoiding unnecessary retention; ensuring data security; limiting and controlling sharing with third parties; providing clear notice to parents and children; and ensuring that the methods used achieve reasonable accuracy. This development demonstrates that age verification is increasingly becoming a central issue on the regulatory agenda at both the federal and state levels in the United States.

Developments in Türkiye

Personal Data Protection Board – Ex Officio Investigation into Digital Platforms

Although there is no specific legislation in Türkiye exclusively dedicated to the protection of children's personal data, the issue remains on the agenda of the authority and other regulatory bodies. Recently, the Turkish Data Protection Authority announced that the Personal Data Protection Board has decided to initiate an ex officio investigation into how children's personal data are processed on social media platforms and what measures are taken to protect them. The investigation - conducted with due regard to the best interests of the child and aimed at safeguarding children from potential risks encountered in digital environments - covers TikTok, Instagram, Facebook, YouTube, X, and Discord.

In addition, the Bilgi Teknolojileri ve İletişim Kurumu (BTK) recently imposed access restrictions on nine live-streaming applications, including Bigo Live, MICO, and SoulChill, pursuant to an access-blocking decision issued by the Ankara 10th Criminal Court of Peace.

Recent regulatory and administrative steps taken to protect children's data privacy demonstrate that this field has become a priority policy area on a global scale. These developments reflect a strong international trend recognizing that children's data is no longer merely a matter of technical compliance, but a fundamental rights and digital safety issue.

Restrictive regulations targeting advertising practices directed at children are also reportedly being planned.

The Protection of Children's Data Requires a Distinct Legal Regime

The Best Interests of the Child

The fundamental assumption of data protection law is that individuals are able to exercise informed control over their personal data. However, children may not fully comprehend the scope and consequences of data processing, may be unable to foresee long-term digital implications, may lack the capacity to assess the legal consequences of contractual and consent mechanisms, and are more susceptible to manipulation and behavioral steering. For this reason, a child's declaration of "free will" is not accorded the same legal weight as that of an adult.

The United Nations Convention on the Rights of the Child recognizes the best interests of the child as a fundamental principle. The reflection of this principle in data protection law is the stricter

scrutiny of processing activities that may pose risks or harm to children. Although the primary objective remains the protection of data privacy, the underlying aim is, more broadly, to safeguard children's psychological, social, and cognitive development.

The Risk of a Long-Term Digital Footprint

Digital traces created during childhood may have significant effects in adulthood on employment opportunities, social reputation, access to education, and even security. While adults may knowingly assume certain risks when consenting to the processing of their data, children generally lack the level of awareness necessary to assess the future implications of such processing. For this reason, children's data carries heightened risk, particularly from a temporal perspective. Digital footprints formed through parental sharing, social media accounts, online gaming activities, educational platforms, and mobile applications may generate long-term data profiles relating to identity, location, behavioral patterns, and interests. Such data is often persistent, may be processed by third parties, and can have lasting implications for an individual's privacy in later years.

The Risk of Profiling and Algorithmic Manipulation

In recent years, the core operating principles of social media platforms have been shaped around behavioral advertising, content recommendation algorithms, and attention economy models. Data collected in relation to children can influence their preferences, attention spans, and consumption habits through content recommendation systems, personalized advertisements, in-game prompts, or algorithmic rankings. Children, who are in a developmentally more vulnerable stage, are more susceptible to data-driven design techniques and dark patterns. For this reason, data processing activities targeting children raise concerns not only from a privacy perspective, but also in terms of behavioral influence.

Legal Capacity and the Consent Dilemma

In data protection law, valid consent must be based on an informed and freely given expression of will. However, children have limited legal capacity, and their ability to discern and understand varies according to age. Consequently, their capacity to make informed choices in the digital environment may be restricted. Platforms possess the technical capability - through advanced data analytics and algorithmic systems - to measure, predict, and influence user behavior. Children, on the other hand, often lack the ability to comprehend how this technical infrastructure operates. Terms of service and privacy policies are typically lengthy and complex documents, and children's ability to understand and evaluate their consequences is limited. Design elements such as notifications, reward mechanisms, infinite scrolling, and gamification techniques are also considered to have a stronger influence on children, who are developmentally more sensitive. For these reasons, many jurisdictions have introduced additional safeguards for the processing of children's personal data, including parental consent requirements for children below a certain age or the direct application of age thresholds.

Global Regulatory Approaches to the Protection of Children's Data

EU General Data Protection Regulation (GDPR)

Article 8 of the General Data Protection Regulation ("GDPR") regulates the age threshold for children's consent in relation to information society services. Where an information society service is offered directly to a child and the processing activity is based on consent as the legal ground, if the child is under the age of 16, such consent is considered valid only if it is given or authorized by the holder of parental responsibility. Member States may lower this age threshold to 13.

Accordingly, within the EU, the applicable age limit varies between 13 and 16 depending on national legislation.

United Kingdom Information Commissioner's Office (ICO)

The Children's Code issued by the Information Commissioner's Office (ICO) represents one of the most advanced regulatory examples globally. This framework goes beyond a consent-based model and directly intervenes in platform design. It introduces obligations such as high privacy settings by default, geolocation switched off by default, restrictions on profiling, prohibition of nudge techniques that operate to the detriment of children, and mandatory data protection impact assessments for high-risk processing activities. The fine imposed on Reddit was based not only on deficiencies in age verification, but also on the failure to conduct a risk assessment specifically concerning children and on inadequacies in the design of its data processing framework. The Reddit decision is significant in demonstrating that merely stating "under 13 is prohibited" is no longer considered sufficient. It reflects an expectation that data controllers processing children's personal data must implement effective, measurable, and technically verifiable safeguards.

United States – Children's Online Privacy Protection Act (COPPA)

In the United States, children's data is regulated under the Children's Online Privacy Protection Act (COPPA), which requires parental consent for users under the age of 13. However, the U.S. approach is not primarily grounded in a fundamental rights perspective; rather, it is based on consumer protection and unfair or deceptive trade practices principles. Enforcement actions by the Federal Trade Commission (FTC), including decisions concerning TikTok and YouTube, have relied on deficiencies in parental consent mechanisms and misleading practices. Nevertheless, the U.S. approach to behavioral advertising remains less stringent than that of the European Union.

Türkiye – Personal Data Protection Law

In Türkiye, Law No. 6698 on the Protection of Personal Data does not contain a specific provision dedicated exclusively to children. The first concrete guidance of the Kişisel Verileri Koruma Kurumu regarding measures to be taken by data controllers for the protection of minors' data can be considered its 2023 decision concerning TikTok. Prior to the recent ex officio investigations initiated against social media platforms, the Board did not have a systemic enforcement practice specifically targeting the protection of children's personal data on such platforms.

Considering global trends and the Board's recent decision to initiate ex officio investigations into social media platforms, developments such as the publication of dedicated guidelines on children's data and the establishment of technical standards for age verification systems are expected in the near future in Türkiye.

The growing expectation placed on platforms to implement "real" age verification mechanisms also gives rise to a serious legal dilemma. Effective age verification typically requires the processing of additional data. Yet one of the core principles of data protection law is data minimization. AI-based age estimation, biometric analysis, and facial recognition technologies are increasingly mentioned as potential solutions for robust age verification; however, these methods may involve the processing of special categories of personal data. The key question therefore becomes: to what extent is it legitimate to process more data in order to protect children?

This issue is likely to become a significant topic of debate in the coming years, both in the context of data protection and AI regulation. Although Türkiye is still at an early stage of this transformation, given the high concentration of child users on digital platforms, regulatory intervention appears inevitable.

Authors:

- https://gun.av.tr/people/begum-yavuzdogan-okumus
- https://gun.av.tr/people/seda-takmaz