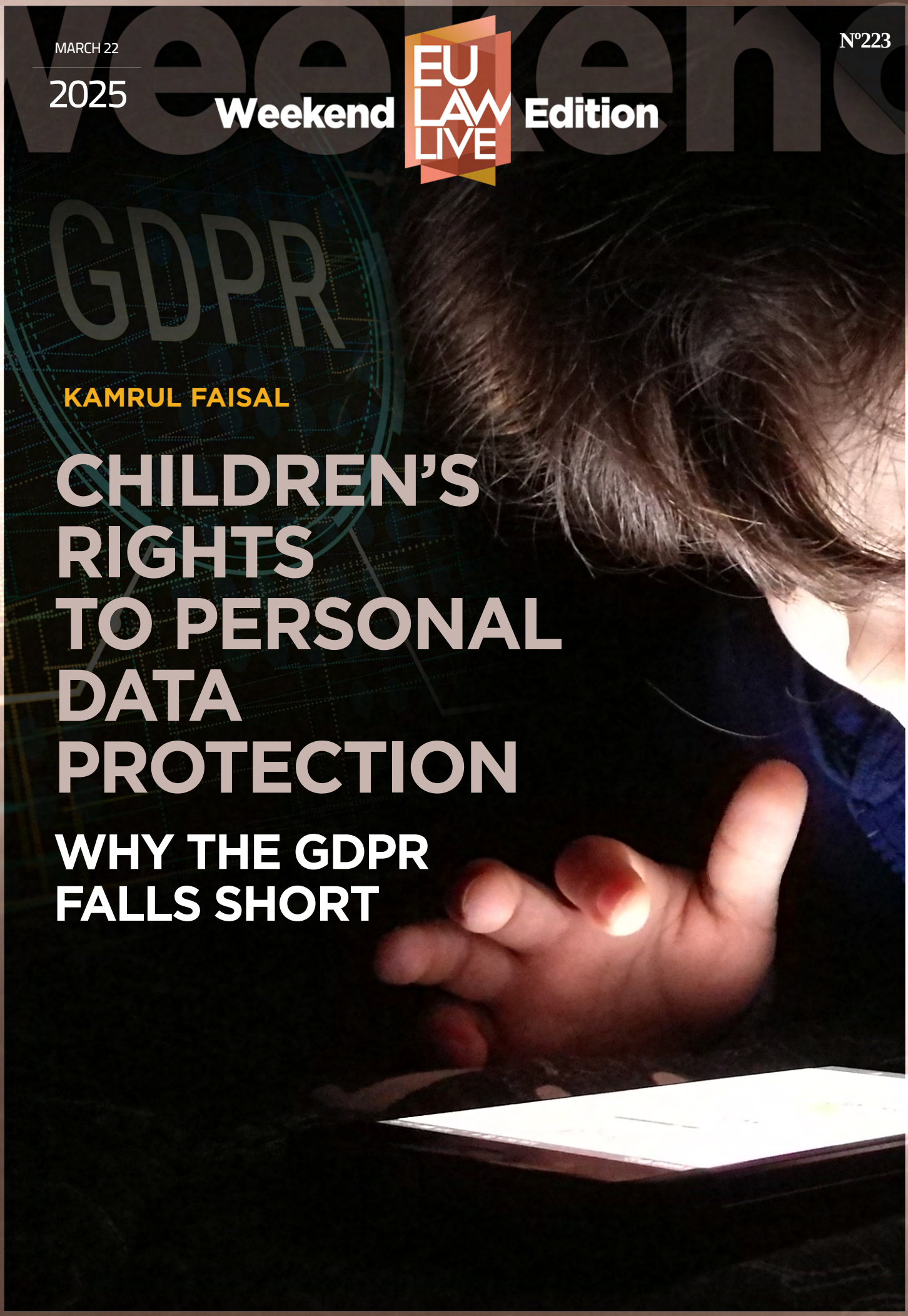
Children’s Rights to Personal Data Protection : Why the GDPR Falls Short

Faisal, Kamrul

2025-03-22
EU Law Live Sociedad Limitada
http://hdl.handle.net/10138/594761
Faisal, K 2025, 'Children’s Rights to Personal Data Protection : Why the GDPR Falls Short', EU law live. Weekend edition. , no. 223. < https://eulawlive.com/weekend-edition/weekend-edition-no223/ >

MARCH 22
2025
Weekend EU LAW LIVE Edition
Nº223



KAMRUL FAISAL

CHILDREN'S RIGHTS TO PERSONAL DATA PROTECTION

WHY THE GDPR FALLS SHORT

Children's Rights to Personal Data Protection
Why the GDPR Falls Short[1]

Kamrul Faisal [2]

1. Introduction: The Promise of the GDPR and its Limitations for Children in the Digital Age

Children today are growing up in a world defined by pervasive digital technologies. From smartphones and social media to online education and gaming platforms, their lives are inextricably linked to a data-driven ecosystem that continuously collects, analyses, monetises, and processes[3] their personal data.[4] This unrelenting datafication—conducted by both private companies and public institutions[5]—subjects children to risks ranging from manipulation and exploitation to the erosion of data protection rights.[6] Compounding this vulnerability is the rise of practices such as *sharenting*[7], where parents unwittingly expose their children's personal data online,[8] such as images, videos, hobbies, interests, date of birth, health information, educational details, and so forth often without considering the long-term consequences.[9] Emerging technologies, including biometric data collection and facial recognition, further magnify these risks, threatening to compromise children's autonomy, dignity, and development.[10]

1. This work was supported by the Generation AI project at the University of Helsinki, funded by the Council for Strategic Research (STN) through the Academy of Finland under grant number 01331393.

2. Kamrul Faisal is a doctoral researcher at the Faculty of Law, University of Helsinki, Finland, specialising in information and communication law, with a particular focus on digital rights, including privacy and personal data protection.

3. Article 4(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), OJ 2016 L 119, p. 1, defines processing of personal data as any activity such as collection, storage, modification, erasure, or transfer that is performed on personal data.

4. Article 4(1) GDPR, *supra* note 3 defines personal data as any information that identifies a human directly or indirectly.

5. Claire Bessant, 'Children, Public Sector Data-Driven Decision-Making and Article 12 UNCRC' 13 *European Journal of Law and Technology* 2, 2022, p. 13.

6. Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable Data Subjects' 37 *Computer Law & Security Review* 1, 2020, p. 5.

7. 'Sharenting' refers to a phenomenon where parents share information about their children online. It often occurs without the child's consent and can lead to data exploitation.

8. Anna Bunn, 'Unwanted Distribution of Children's Images and the Right to Development', 84 *The Modern Law Review* 334, 2021, pp. 368–370.

9. Anica Čulo Margaletić and Barbara Preložnjak, 'Children's Right to Privacy in the Digital Age', X *Intereulaweast* 2, 2023, pp. 81-100; Natasha Kravchuk, 'Privacy as a New Component of "The Best Interests of the Child" in the New Digital Environment', 29 *The International Journal of Children's Rights*, 2021, pp. 99-121.

10. Steven Feldstein, 'State Surveillance and Implications for Children' *Good Governance of Children's Data Project*, Issue Brief 1, 2020, p. 7.

The General Data Protection Regulation (GDPR), hailed as a landmark in global data protection law,[11] was designed to address the challenges posed by modern data practices.[12] Entering into force in 2018, it grants individuals greater control over their personal data,[13] emphasising data processing principles like consent, transparency, and accountability. Recognising children as vulnerable data subjects, the GDPR includes provisions specifically aimed at safeguarding their data in specific areas, such as obtaining parental consent.

However, these provisions fall short of addressing the unique and evolving vulnerabilities children face in the digital age.[14] This piece examines the GDPR's limitations in protecting children's personal data, emphasising inconsistent definitions, consent issues, and controller accountability.

2. Conceptualising Children under the GDPR and its Shortcomings

To provide extended protection for children's personal data, the GDPR acknowledges children as 'vulnerable individuals' (Recital 75), primarily because they may lack the capacity to fully comprehend the risks associated with data processing concerning them (Recital 38), making them a special type of data subject,[15] entitled to receive extended protection[16] compared to adults who are assumed to be reasonably well-informed, rationale and circumspect.[17] Children are generally viewed as vulnerable due to their cognitive, emotional, and moral immaturity, along with their limited knowledge of the world. Both internal (related to age, competence, and experience) and external factors (related to complex market strategies) contribute to their vulnerabilities,[18] which makes children inherently vulnerable.[19] This vulnerability makes them heavily reliant on others to meet their basic needs and be protected from risks to their well-being,[20] and other rights.[21] The GDPR's recognition of this vulnerability is a positive step to protect their rights and freedoms related to personal data protection. However, it does not translate effectively into comprehensive protection mechanisms due to the definition that children receive under the law.

11. Thomas Linden and others, 'The Privacy Policy Landscape After the GDPR', 2020 *Proceedings on Privacy Enhancing Technologies* 1, 2020, p. 47.

12. Article 2, GDPR, *supra* note 3.

13. Manon Oostveen and others, Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? (Mor Bakhoum and others Eds.), Springer-Verlag Berlin, 2018 p. 79.

14. Gianclaudio Malgieri and Gloria González Fuster, 'The Vulnerable Data Subject: A Gendered Data Subject?' 13 *European Journal of Law and Technology* 1, 2022, p. 1.

15. Article 4(1) GDPR, *supra* note 3 impliedly defines data subjects as a living, identified or identifiable natural person to whom personal data relates to.

16. Article 29 Data Protection Working Party, 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)', 2009, p. 6.

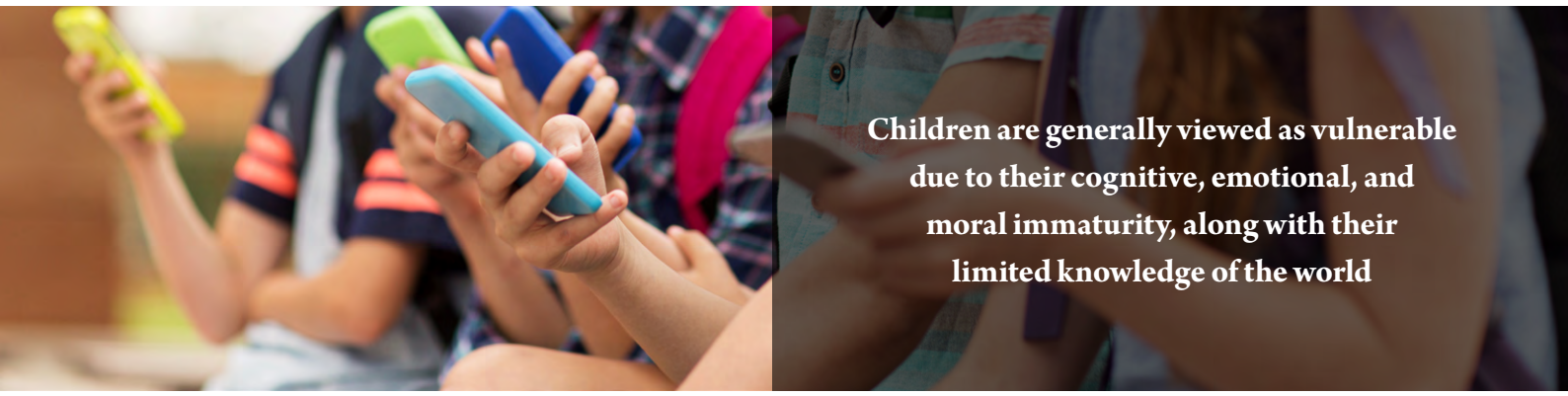
17. Malgieri and González Fuster (n 14), p. 25.

18. Oostveen and others (n 13), p. 368.

19. Alexander Bagattini, 'Children's Well-Being and Vulnerability' 13 *Ethics and Social Welfare*, 2019, p. 211.

20. Colin Macleod, 'Paradoxes of Children's Vulnerability' 13 *Ethics and Social Welfare* 261, 2019, p. 264.

21. Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR When Vulnerable People Use Smart Devices' 12 *International Data Privacy Law* 113, 2022, p. 113.



While defining children, the GDPR considers anyone below the age of 16 as a child, leaving the possibility for the Member States to lower the age to no less than 13.[22] Thus, the GDPR provides a combination of dynamic and static definitions of children which can be between 13 and 16.[23] Consequently, there are variations definitions of children throughout the Union providing different levels of protection to different groups of people. To mention a few examples, for data protection purposes, Spain considers anyone below 14 years old as a child,[24] whereas the Netherlands and Hungary consider anyone under 16 years old,[25] and Finland considers anyone below 13 years of age as a child[26] to provide children with specific protections under the GDPR. What this means *inter alia* is that in Finland, 13-year-olds may not receive child-specific protections under the GDPR, though in Spain, Netherlands, and Hungary—they do, creating legal uncertainties and disharmonisation in protecting children's personal data throughout the Union.

This approach is inconsistent with the developmental realities or evolving capacities of children,[27] as it assumes generally that no child has the cognitive capacity to make informed, autonomous decisions about their personal data.[28] In reality, an empirical study reveals that children aged between 7 and 13 in the UK have the capacity to generate data privacy warnings for each other,[29] meaning children between the ages of 7 and 13, for instance, may possess the intellectual ability to understand data privacy risks. Another empirical study endorses that children

22. Article 8 GDPR, *supra* note 3.

23. Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' 26 *Information & Communications Technology Law* 146, 2017; Kamrul Faisal, 'Certain Legal Aspects of Children's Right to Protect Personal Data in the Context of AI under the European Union Data Protection Laws' in Päivi Korpisaari (Ed.), *Vapaita sanoja: Viestintäoikeuden vuosikirja 2022*, Forum Iuris, 2023.

24. Macenaite and Kosta (n 23), pp. 152–155.

25. *ibid.*

26. Section 5, Data Protection Act 1050/2018.

27. Bagattini (n 19), pp. 214–215.

28. Malgieri and Niklas (n 6), p. 5.

29. John Dempsey and others, 'Children Designing Privacy Warnings: Informing a Set of Design Guidelines' 31 *International Journal of Child-Computer Interaction* 1, 2022, p. 15.

aged between 11 and 18 are interested in knowing how their data is processed and want their voices to be heard.[30] This leaves a significant gap in the GDPR's protection of children, as it fails to recognise the need for differentiated approaches based on a child's developmental stage. A 13-year-old's abilities are not the same as that of a 5-year-old, though they may use the same online services.[31]

It indicates that children of different ages demonstrate different vulnerabilities based on their ages in the digital ecosystem, and the general GDPR notion that 'they are less aware of the risks, consequences, and safeguards' concerning the processing of their personal data[32] does not help protect all children's data protection rights meaningfully. Rather, it risks interfering with their data protection rights by failing to consider their growing and/or grown autonomy as well as interfering with other rights such as the right to participate in decision-making that affects them as provided to them under Article 12 of the United Nations Convention on Rights of a Child (UNCRC)[33] to which the European Union (EU) is a party.[34]

3. The GDPR's Current Approach to Children's Personal Data Protection and its Limitations

Among child-specific provisions, the issue of consent is central to the GDPR's approach to protecting children's data.[35] The GDPR outlines specific protections for children under Articles 8 and 12, mandating that controllers[36] seek parental consent for processing children's data, emphasising transparency. Platforms are mandated to inform children and their parents about data collection and processing types and purposes, ensuring that only necessary data are processed. Further, as per Article 8 of the GDPR, a child cannot consent to the processing of personal data, instead, anyone having parental responsibility is empowered to consent on their behalf. While this requirement is crucial, it is not without its flaws, particularly when applied to children, for several reasons.

First of all, the Regulation's reliance on parental consent as a primary safeguard is problematic due to two reasons. First, the GDPR assumes that children's consent cannot be meaningfully obtained,[37] since children cannot make free and informed choices[38] and cannot meet the conditions of providing consent. Thus, the GDPR's approach does not account for the growing autonomy and evolving capacity of those in the adolescent age range, to understand

30. Bessant (n 5), p. 3.

31. Feldstein (n 10), p. 4.

32. Recital 38, GDPR, *supra* note 3; Kamrul Faisal, 'Protecting Our Children in a Digital Age: How the GDPR and EU AI Act Step Up to Keep Kids Safe Online' *Perustuslakiblogi: Suomen valtiosääntöoikeudellisen seuran ajankohtaispalsta*, 11 November 2024.

33. Bessant (n 5), p. 16.

34. European Commission, 'EU Action on the Rights of the Child', accessed 14 January 2025.

35. Bart HM Custers and others, 'The Role of Consent in an Algorithmic Society. Its Evolution, Scope, Failings, and Re-Conceptualization' in E Kostas, R Leenes and I Kamara (Eds.), *Research Handbook on EU data protection*, Edward Elgar Publishing, 2022, pp. 472–473.

36. Article 4(7) GDPR, *supra* note 3 defines controller as any authority who determines the means and purpose of processing personal data.

37. Ananya Karthik, 'Reimagining the Data Subject in GDPR' 1 *GRACE: Global Review of AI Community Ethics* 1, 2023, p. 6.

38. *ibid.*, p. 1.

and manage their data privacy. Second, it assumes that parents are always aware of and capable of managing the complexities of digital data processing.[39] In reality, they are not. Parents often compromise their children's privacy through sharenting, underestimating the reach and permanence of shared data.[40] Despite being primary defenders, they may lack understanding of data protection, inadvertently exposing children to risks like identity theft, targeted advertising, and unwanted surveillance,[41] highlighting their inability to fully protect children's data.

Next, the age threshold for parental consent is inconsistent across the EU—between 13 and 16 years. This variation leads to a fragmented approach to children's data protection, where a child deemed capable of consenting in one country may not be recognised as such in another.

The GDPR assumes that children's consent cannot be meaningfully obtained, since children cannot make free and informed choices and cannot meet the conditions of providing consent

As highlighted by contemporary scholars and experts, consent under the GDPR often fails to be informed in the case of children.[42] Children's limited understanding of the risks associated with data processing means that they cannot make fully autonomous decisions regarding their personal data.[43] The GDPR's reliance on parental consent further complicates the issue.[44]

39. Macleod (n 20).

40. Margaletić and Preložnjak (n 9), pp. 95–96.

41. United Nations Committee on the Rights of the Child, 'General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment', CRC/C/GC/25, 2021, pp. 11–13.

42. Custers and others (n 35); Karthik (n 37).

43. Karthik (n 37), p. 6.

44. Kravchuk (n 9), p. 117.

Overall, the GDPR lacks specific provisions to tackle such emerging risks, and its data protection tools are insufficient to address the complexities of digital platforms that children engage with daily.

Nevertheless, the GDPR provides a safeguard for situations where parental consent is not required, such as when children seek preventive or counseling services directly. However, this provision is limited in scope and does not address the vast majority of data processing activities that involve children. The GDPR's accountability framework comprises providing appropriate technical and organisational measures,[45] data protection and by design and by default, among others,[46] placing the burden on controllers to ensure that services are designed in a way that respects children's data protection rights, yet the regulation lacks specific guidance on how this responsibility should be fulfilled in practice.

4. The Role of Controllers and the Need for Stronger Oversight

Another significant shortcoming of the GDPR is its failure to place sufficient responsibility on data controllers when it comes to the processing of children's data.[47] The GDPR assumes children lack understanding, yet fails to ensure controllers adequately address this by providing clear, accessible information. For example, cases like TikTok's 'public-by-default' settings, inadequate age verification,[48] live video streaming in classroom settings,[49] and mandatory biometric data collection in providing identity card settings[50] highlight unclear guidance for protecting children's data. The Court of Justice of the European Union (CJEU) rulings emphasise gaps in balancing children's growing capacities, security, and privacy rights, particularly in marketing, profiling, and public data disclosures. These examples reveal the GDPR's insufficient differentiation based on age, lack of robust safeguards, and failure to ensure children's best interests are consistently prioritised across diverse contexts. Moreover, enforcement is fragmented, and emerging risks like

The GDPR provides a safeguard for situations where parental consent is not required, such as when children seek preventive or counseling services directly

45. Article 24, GDPR, *supra* note 3.

46. Lachlan Urquhart, Tom Lodge and Andy Crabtree, 'Demonstrably Doing Accountability in the Internet of Things' 27 *International Journal of Law and Information Technology* 1, 2019.

47. Feldstein (n 10), p. 2.

48. European Data Protection Board, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art 65 GDPR), 2 August 2023.

49. Judgment of the Court of Justice of 30 March 2023, *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums* (C-34/21, ECLI:EU:C:2023:270, para 26).

50. Judgment of the Court of Justice of 21 March 2024, *RL v Landeshauptstadt Wiesbaden*, (C-61/22, ECLI:EU:C:2024:251, paras 26, 27).

targeted advertising[51] are inadequately covered.[52] Ultimately, controllers often neglect GDPR provisions specific to children, exploiting their vulnerabilities.

Furthermore, the GDPR lacks robust oversight mechanisms to ensure that controllers are held accountable for their treatment of children's data. While the Regulation provides for administrative fines and penalties,[53] these sanctions are often not enough to deter data controllers from engaging in harmful data practices.[54] The European Data Protection Board (EDPB) has issued guidelines on the processing of children's data,[55] but these guidelines are not legally binding, and there is no effective enforcement mechanism to ensure compliance.

Another significant shortcoming of the GDPR is its failure to place sufficient responsibility on data controllers when it comes to the processing of children's data

Stronger oversight is essential to ensure that data controllers are held accountable for their treatment of children's data. This could involve more proactive monitoring by supervisory authorities, greater transparency in the way children's data is used, and clearer standards for what constitutes acceptable data processing practices in the context of children.[56] Ultimately, controllers must be required to take a more active role in protecting children's privacy and ensuring that their personal data is not misused or exploited.

51. Targeted advertising refers to data-driven techniques that analyse users' behaviours, preferences, and habits to deliver personalised ads. When applied to children, this practice risks undermining their autonomy, influencing preferences prematurely, and hindering healthy development. Profiling using predictive analytics raises concerns about trust and data privacy in marketing. For further reading on targeted advertising, see: Mara Paun, 'Learning from Internal Models of Reality: The Case of Data Protection and Consumer Protection in Financial Services', 1 *TILT Law & Technology Working Paper*, 2021; Gianclaudio Malgieri, 'In/Acceptable Marketing and Consumers' Privacy Expectations: Four Tests from EU Data Protection Law' 40 *Journal of Consumer Marketing* 209, 2023; Oostveen and others (n 13); Valerie Verdoodt and Eva Lievens, 'Targeting Children with Personalised Advertising: How to Reconcile the (Best) Interests of Children and Advertisers' in Gert Vermeulen and Eva Lievens (Eds.), *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data*, Maklu, 2017.

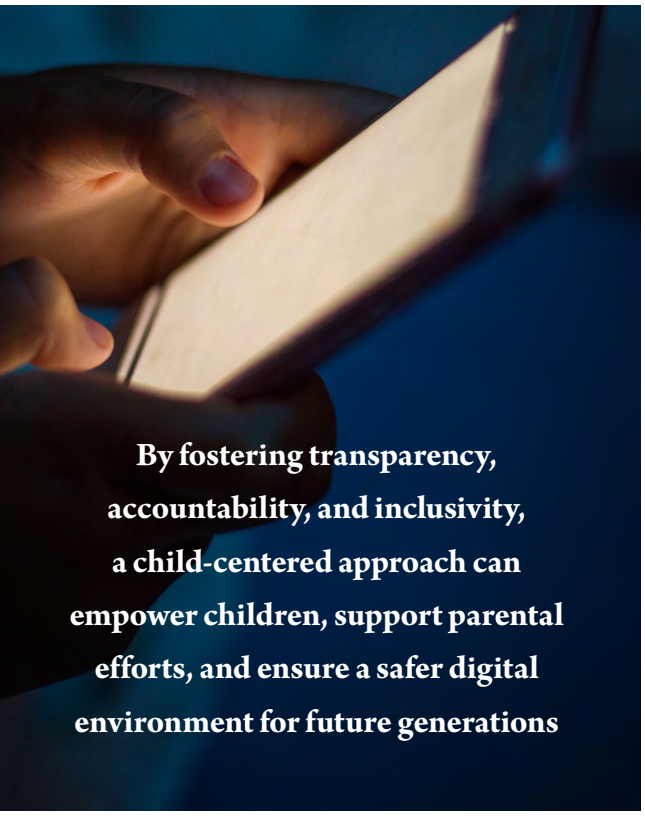
52. Verdoodt and Lievens (n 51), p. 335.

53. Kamrul Faisal, 'Decoding Vulnerability within the GDPR', *CiTiP Blog*, 20 February 2024.

54. Mona Naomi Lintvedt, 'Putting a Price on Data Protection Infringement' 12 *International Data Privacy Law* 1, 2022, p. 1.

55. European Data Protection Board (EDPB), 'Guidelines 8/2020 on the Targeting of Social Media Users', 2 September 2020, para 16.

56. Feldstein (n 10), pp. 5–6.



5. Moving Forward: A Child-Centered Approach to Data Protection

To better protect children in the digital age, data protection frameworks must adopt a child-centered approach that acknowledges children's evolving capacities while addressing their unique vulnerabilities. Moving beyond the limitations of the GDPR, regulators should introduce clearer, enforceable guidelines requiring data controllers to provide age-appropriate, accessible information. Safeguards such as mandatory age verification, robust parental education, and mechanisms for children's meaningful participation in decisions about their data are essential. Oversight bodies must proactively monitor compliance, impose stricter penalties for violations, and prioritise children's best interests across all data practices. By fostering transparency, accountability, and inclusivity, a child-centered approach can empower children, support parental efforts, and ensure a safer digital environment for future generations.

Subscription prices are available upon request. Please contact our sales department for further information at

subscriptions@eulawlive.com

ISSN

EU Law Live **2695-9585**
EU Law Live Weekend Edition **2695-9593**


EU
LAW
LIVE