Advance online publication https://doi.org/10.5204/lthj.3821

Reforming Child Consent Under the GDPR: Towards a Harmonised, Risk-Aware and Child-Centred Framework

Kamrul Faisal
University of Helsinki, Finland

Abstract

This article examines the current framework governing child consent under the European Union's (EU) General Data Protection Regulation (GDPR). It identifies significant gaps that hinder effective protection of children's personal data. Three principal shortcomings were found in the research: divergent national age thresholds for digital consent; unclear and inconsistently enforced parental consent verification obligations; and insufficient recognition of children's evolving capacity.

Through a comprehensive analysis, the study proposes a reformed, child rights-based model that emphasises three core pillars: harmonised age thresholds, risk-calibrated parental consent verification and operationalising children's growing decision-making capacities. The article advocates for clearer regulatory guidance, context-sensitive consent mechanisms and enhanced digital literacy initiatives to empower children and parents. It further advocates systematic integration of Child Rights Impact Assessments to complement Data Protection Impact Assessments in high-risk contexts. These measures aim to align legal obligations with technological realities, enhance transparency and foster participatory data governance that treats children as active rights-holders.

The proposed framework seeks to reconcile protective imperatives with empowerment objectives, delivering greater legal certainty for controllers while advancing fairness, proportionality and inclusivity in the EU's digital single market. This approach offers a principled pathway towards ensuring that children's data rights are safeguarded not only through stronger protections but also by recognition of their agency within the contemporary digital ecosystem.

***Keywords**:* Child consent; GDPR, data protection; parental consent verification; children's evolving capacity.

1. Introduction: Rethinking Children's Digital Consent Under the GDPR

Children are identified in this context as data subjects – that is, identified or identifiable natural persons whose personal data are being collected or processed.[1] Within the digital environment, children are increasingly interacting with a wide array of digital services commonly known as information society services (ISS),[2] including social media platforms,[3] e-learning tools,[4] smart toys[5] and streaming applications.[6] These service providers typically function as controllers, meaning that they determine

[1] Article 4(1), Regulation (EU) 2016/679.
[2] Directive (EU) 2015/1535.
[3] Margaletić, "Children's Right to Privacy," 82.
[4] Digital Futures Commission, Governance of Data.
[5] Fosch-Villaronga, "Toy Story or Children Story?" 133.
[6] Court of Justice of the European Union, *Case C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums*, para 26.

the purposes and means of the processing of personal data.[7] In this context, processing encompasses any operation performed on personal data, including collection, storage, use or dissemination.[8] The term 'personal data' refers to any information relating to an identified or identifiable child, such as names, location data, online identifiers or characteristics specific to their physical, physiological or social identity.[9] While providing services, these controllers routinely collect and process vast amounts of children's personal data. While these technologies offer educational and social benefits,[10] they also expose children to opaque profiling, behavioural targeting and surveillance practices that raise serious data protection concerns.[11] Regulatory actions against platforms such as YouTube and TikTok[12] underscore the urgency of ensuring that children's rights are meaningfully protected in digital environments.

To protect children from unlawful processing of their personal data, the European Union (EU) has established a legal data-protection framework, providing rights-based[13] and risk-based approaches,[14] backed by administrative fines[15] and other enforcement mechanisms.[16] The rights-based approach emphasises the protection of individuals' fundamental rights and freedoms – such as privacy and data protection – while a risk-based approach focuses on identifying and addressing potential harms to the rights that may arise from data processing.[17] These dual but interdependent approaches are firmly grounded in the Charter of Fundamental Rights (the Charter),[18] the Treaty on the Functioning of the European Union (TFEU)[19] and the European Convention on Human Rights (ECHR).[20] In addition, the United Nations Convention on the Rights of the Child (UNCRC),[21] to which the EU adheres,[22] protects children's data privacy. Although the UNCRC does not explicitly reference data protection, its right to privacy under Article 16 and its digital interpretation in General Comment No 25 affirm protections applicable to children online.[23]

The General Data Protection Regulation (GDPR)[24] operationalises these commitments, recognising children as a group requiring enhanced safeguards.[25] In particular, Article 8 of the GDPR – along with Recitals 38 and 75 – establishes conditions for obtaining consent when children access ISS. Where a child is below the nationally established age threshold, ranging between 13 and 16 years, valid consent must come from an individual holding parental responsibility.[26]

However, this framework presents several challenges. First, the variable age thresholds across member states create legal fragmentation, undermining harmonisation and complicating compliance for cross-border service providers.[27] Second, the

[7] Article 4(7), Regulation (EU) 2016/679.
[8] Article 4(2), Regulation (EU) 2016/679.
[9] Article 4(1), Regulation (EU) 2016/679.
[10] Morehouse, "The Kids are Not Alright"; Thompson, "How Videogames Like Minecraft."
[11] Oostveen, Personal Data in Competition; Malgieri and González Fuster, "The Vulnerable Data Subject"; Bessant, "Children, Public Sector Data-Driven Decision-Making."
[12] BBC News, "YouTube Fined $170m"; European Data Protection Board (EDPB), Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art 65 GDPR).
[13] Recital 1, Regulation (EU) 2016/679.
[14] Gonçalves, "The Risk-Based Approach."
[15] Kosta, "Article 8. Conditions Applicable to Child's Consent," 362.
[16] Faisal, "Decoding Vulnerability."
[17] Gonçalves, "The Risk-Based Approach," 139.
[18] Articles 8 and 24, Official Journal of the European Union, Charter of Fundamental Rights of the European Union.
[19] Article 16, Consolidated version of the Treaty on the Functioning of the European Union.
[20] Article 8, Council of Europe, European Convention on Human Rights.
[21] United Nations, Convention on the Rights of the Child.
[22] European Parliament, "Children's Rights in the EU."
[23] United Nations, Convention on the Rights of the Child; United Nations Committee on the Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment."
[24] Regulation (EU) 2016/679.
[25] Regulation (EU) 2016/679; Faisal, "Children's Rights."
[26] European Data Protection Board (EDPB), Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art 65 GDPR); Kosta, "Article 8. Conditions Applicable to Child's Consent"; Kosta, "Article 7. Conditions for Consent"; European Data Protection Supervisor, Data Protection.
[27] Verdoodt, "Safeguarding the Child's Right to Privacy"; Macenaite, "Consent for Processing Children's Personal Data"; European Union Agency for Fundamental Rights, "Consent to Use Data on Children."

reliance on parental digital literacy to act in the child's best interests is not functioning very well.[28] Parental over-sharing and surveillance practices may infringe on children's rights to privacy, expression and participation.[29]

Additionally, Article 8 does not adequately reflect the evolving capacities of children, as articulated in Article 5 of the UNCRC.[30] This principle acknowledges that, as children – particularly adolescents – develop greater maturity and understanding,[31] they should progressively be empowered to exercise autonomy in decisions affecting them, including those related to the processing of their data.[32] This lack of differentiation among toddlers, children in middle childhood and adolescents contributes to a model that can over-protect younger children while constraining the autonomy of older minors, contrary to both EU data protection principles and international children's rights norms.[33] In light of these limitations, Article 8's current consent framework lacks coherence, clarity and sensitivity to developmental differences. A revised model is needed to move the privacy law forward[34] – one that aligns with children's digital realities, legal protections and evolving capacities.
This study asks how Article 8 of the GDPR can be reformed to establish a harmonised, clear and child-rights-based consent model. The study employed doctrinal legal analysis,[35] examining the text, structure and interpretation of the GDPR, differing member states' laws, relevant case law and regulatory guidance. Secondary sources, including previous scholarship and comparative legislative models, informed the critique. Normative evaluation grounded in UNCRC principles was used to develop reform proposals integrating harmonisation, proportionality and recognition of children's evolving capacities.

The article proceeds as follows: Section 2 evaluates the GDPR's current consent model; Section 3 identifies five key fault lines in Article 8; Section 4 introduces a reformed, child-centered consent framework; Section 5 discusses its legal and ethical implications; and Section 6 concludes with recommendations for future research.

2. An Analysis of the GDPR's Consent Mechanism for Processing Children's Personal Data

While Article 8 of the GDPR was designed to introduce a tailored legal regime for protecting children's personal data in the context of ISS, it suffers from critical structural and interpretive flaws[36] that undermine its effectiveness, legal coherence and harmonisation across the EU.

2.1 Legal Structure of Article 8 of the GDPR

As a *lex specialis* within the broader GDPR framework, Article 8 applies specifically when consent is the lawful basis for processing personal data under Article 6(1)(a),[37] in case the offered service qualifies as an ISS and is directed to a child. The provision operationalises Recital 38, which emphasises children's need for specific protections due to their limited awareness of risks related to personal data processing.

2.1.1 Article 8(1): Age Threshold and the Nature of ISS

Article 8(1) sets a default age of 16 years as the threshold for children to provide valid, independent consent. Member states may, however, legislate a lower age – although no less than 13 years – leading to a partially harmonised system. This flexibility, while meant to respect national subsidiarity, has fragmented legal protections across the EU, contradicting the GDPR's goal of a uniform digital market.[38]

The notion of consent is defined in Article 4(11) of the GDPR as a 'freely given, specific, informed and unambiguous' expression of will, communicated through a clear affirmative action. In turn, Article 7 of the GDPR stipulates that consent must be intelligible, distinguishable from other matters and withdrawable at any time.[39] These criteria apply equally to adults and

[28] Kravchuk, "Privacy as a New Component"; Feldstein, "State Surveillance"; Land, "Sharenting"; Morehouse, "The Kids are Not Alright"; Article 29 Data Protection Working Party, "Opinion on the Use of Location Data with a View to Providing Value-Added Services."
[29] Official Journal of the European Union, Charter of Fundamental Rights of the European Union; United Nations, Convention on the Rights of the Child; Tobin, "Understanding Children's Rights"; Faisal, "Children's Rights," 6.
[30] United Nations, Convention on the Rights of the Child; Dethloff, "Families and the Law."
[31] Livingstone, "Conceptualizing Age-Appropriate Social Media," 7.
[32] Margaletić, "Children's Right to Privacy," 96.
[33] Official Journal of the European Union, Charter of Fundamental Rights of the European Union; United Nations, Convention on the Rights of the Child.
[34] Solove, "Introduction," 1882.
[35] Hutchinson, "Doctrinal Research," 17.
[36] Feiler, "Chapter II – Principles," 91.
[37] Kosta, "Article 8. Conditions Applicable to Child's Consent," 359.
[38] Verdoodt, "Safeguarding the Child's Right to Privacy"; Macenaite, "Consent for Processing Children's Personal Data."
[39] Article 7, Regulation (EU) 2016/679.

children, though children are presumed to have more difficulty understanding the consequences of consent, necessitating special safeguards.[40]

To fall under Article 8, the digital service must qualify as an ISS, as defined under Directive (EU) 2015/1535. An ISS is a service:

- provided for remuneration, including consideration for services[41] through indirect monetisation, such as advertising[42]
- offered at a distance, meaning the provider and the user are not physically present together[43]
- by electronic means, for instance, when it is sent and received using electronic devices that process, store, and transmit the data through technologies like the internet, radio waves, or optical signals,[44] and
- at the request of the recipient, such as the user, by clicking a link or submitting a form online.[45]

This broad definition of an ISS encompasses a wide array of platforms[46] commonly accessed by children, including educational apps such as Duolingo for Schools, Google Classroom, social networks such as TikTok, Instagram, YouTube Kids, gaming environments, video streaming platforms including Disney+ and Netflix Kids, and smart toys. These platforms fulfil all ISS criteria by offering services electronically, at a distance and upon user request; they are typically monetised – directly or indirectly – through subscriptions or advertising, fulfilling all four conditions of an ISS, and thereby fall within the regulatory scope of Article 8 concerning the processing of children's personal data. These services contribute to the so-called datafication of childhood,[47] whereby children's behaviours, preferences and identities are continuously collected and processed, often beyond their or their parents' understanding or control.

The phrase 'offered directly to a child' under Article 8 of the GDPR is not explicitly defined, leading to interpretative uncertainty. However, interpretative guidance – most notably from the former Article 29 Data Protection Working Party (WP29) and subsequently the European Data Protection Board (EDPB)[48] – indicates that the provision encompasses not only services specifically targeted at children but also general audience services where it is reasonably foreseeable that a significant proportion of users will be children.[49] This foreseeability threshold implies that controllers cannot ignore clear evidence of child engagement; where they become aware, or ought reasonably to be aware, that a user is a child, the Article 8 consent requirements are triggered.

The inclusion of the qualifier 'offered directly to a child' signals that Article 8 is not intended to cover all ISS indiscriminately. For instance, where an ISS provider clearly states, through age declarations or contractual terms, that its service is intended only for users aged 18 and above, and such a statement is not contradicted by other factors such as the nature of the content, marketing strategy, or audience analytics, the service will not generally be regarded as being offered directly to a child.[50] This interpretation allows for the exclusion of certain services from Article 8's parental consent obligations, while placing the onus on controllers to ensure that their content, design choices and commercial practices do not indirectly target or significantly appeal to children.

In its analogous regulatory context,[51] the US Children's Online Privacy Protection Act (COPPA)[52] employs its parental consent rules in either circumstance: (1) when online services are 'directed to children', or (2) when the controller has 'actual knowledge' of processing children's data.[53] The US Federal Trade Commission (FTC) – the primary COPPA enforcement

[40] Recitals 38 and 58, Regulation (EU) 2016/679; Malgieri, "Vulnerable Data Subjects."
[41] Court of Justice of the European Union, *Case 263/86, Belgian State and René Humbel and Marie-Thérèse Humbel, née Edel*, para 17.
[42] Court of Justice of the European Union, *Case 352/85, Bond van Averteerders and Others and The Netherlands State*, paragraph 13,16.
[43] Kosta, "Article 8. Conditions Applicable to Child's Consent"; Directive (EU) 2015/1535.
[44] Kosta, "Article 8. Conditions Applicable to Child's Consent"; Directive (EU) 2015/1535.
[45] Kosta, "Article 8. Conditions Applicable to Child's Consent"; Directive (EU) 2015/1535.
[46] Macenaite, "Consent for Processing Children's Personal Data," 171.
[47] Bessant, "Children, Public Sector Data-Driven Decision-Making"; European Data Protection Board (EDPB), "Guidelines 8/2020 on the Targeting of Social Media Users"; Malgieri, "In/Acceptable Marketing"; Court of Justice of the European Union, Opinion of Advocate General Pitruzzella delivered on 27 January 20221 Case C-817/19 *Ligue des droits humains v Conseil des ministres*; Zampino, "Book Review Deborah Lupton The Quantified Self."
[48] European Data Protection Board (EDPB), "Guidelines 05/2020 on Consent under Regulation 2016/679."
[49] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679," 25.
[50] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679," 25.
[51] Macenaite, "Consent for Processing Children's Personal Data," 194–195.
[52] US Congress, Children's Online Privacy Protection Act 15 USC §§ 6501–6506.
[53] Feiler, "Chapter II – Principles," 91.

authority[54] – offers a detailed set of indicators for determining child-directed status, including the service's subject matter, visual style, language, the use of child celebrities, advertising practices and audience metrics.[55] Although grounded in a different legal tradition, this list of factors provides a useful illustration of the types of evidentiary cues that could inform an EU determination of whether a service is 'offered directly to a child'.

The absence of definitive interpretative rulings leaves scope for legal uncertainty, particularly for mixed-audience platforms where children may access services in practice despite stated age restrictions. Until authoritative guidance emerges, controllers face a compliance environment in which 'offered directly to a child' functions as both a normative boundary and a factual inquiry, requiring careful assessment of the nature of the service, its presentation and its foreseeable audience.

While Article 8(1) seeks to balance child autonomy with parental oversight, the provision's lack of precision on age thresholds and applicability to borderline ISS weakens its legal clarity and consistent application.

2.1.2 Article 8(2): Verifying Parental Consent

Article 8(2) places an obligation on controllers to make 'reasonable efforts' using available technology to verify that consent is given or authorised by a person holding parental responsibility, where the child is below the applicable age threshold.[56] This procedural requirement is essential to ensure the legitimacy of consent obtained under Article 8(1). While the GDPR does not define 'reasonable efforts' or 'available technology', the WP29 Guidelines on Consent provide some interpretative clarity. According to the WP29, the reasonableness of verification efforts should be assessed in light of the specific risks posed by the processing, the nature of the service and the technologies available at the time.[57] Controllers are expected to employ verification methods that are effective, accessible and proportionate, ensuring sufficient certainty about parental authorisation without creating excessive barriers or resorting to unnecessarily intrusive measures. The concept of 'available technology' thus functions as a contextual benchmark, requiring controllers to adapt verification mechanisms to current technological capabilities while balancing accuracy, practicality, and privacy.

Moreover, applying the provision to all age groups, ranging from below 13 to 16 years risks limiting children's autonomy. These introduce considerable interpretive leeway, risking inconsistent implementation across sectors and member states.

Although this flexible, risk-based approach promotes proportionality, the absence of a uniform standard dilutes the effectiveness of enforcement and opens the door for platforms to adopt minimal compliance strategies.

2.1.3 Article 8(3): Interaction with National Contract Law

Article 8(3) clarifies that the rules on consent for data processing under Article 8 do not override or alter national laws on contractual capacity. This doctrinal separation acknowledges that the ability to consent to data processing under GDPR is legally distinct from the ability to enter into enforceable contracts – a matter reserved for member states.

This provision preserves the diversity of contract law across the EU, but introduces practical complexity. For example, a child aged 15 may lawfully consent to data processing in one member state, yet be unable to enter into a service contract without parental approval in another.[58] This dichotomy complicates the legal obligations of controllers, who must comply with both data-protection and contractual requirements when offering ISS to minors.

While Article 8(3) avoids legal conflation, it nonetheless exposes a gap in harmonisation, particularly in digital contexts where service access and data processing are closely intertwined.

[54] Section 6502(b)(c), US Congress, Children's Online Privacy Protection Act 15 USC §§ 6501–6506.
[55] Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions."
[56] Regulation (EU) 2016/679; European Data Protection Board (EDPB), "Guidelines 8/2020 on the Targeting of Social Media Users."
[57] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679"; Kosta, "Article 8. Conditions Applicable to Child's Consent in Relation to Information Society Services."
[58] Kosta, "Article 8. Conditions Applicable to Child's Consent," 360.

2.2 Structural Fault-Lines in Article 8

Despite its child-protective objectives, a detailed analysis of Article 8 reveals several fault-lines that hinder its practical enforcement and legal consistency:

1. *Fragmented age thresholds across member states.* The discretion given to member states to lower the age of consent between 'below 13' and 16 has resulted in a patchwork of national rules, undermining cross-border consistency and complicating compliance for ISS providers.[59]
2. *Unclear standards for 'reasonable efforts' and 'available technology'.* The terms 'reasonable efforts' and 'available technology' lack a legal benchmark, leading to varied interpretations of what constitutes sufficient parental verification. This ambiguity undermines uniform protection and encourages regulatory arbitrage.[60]
3. *Over-reliance on parental consent.* The framework vests too many responsibilities on parents, assuming they are informed, rational actors. However, evidence suggests that parents may lack digital literacy, act under social pressure or unknowingly compromise their children's data through 'sharenting' and other behaviours.[61]
4. *Neglect of children's evolving capacity.* Article 8 does not adequately accommodate the growing agency and digital competence of older children and adolescents, resulting in a one-size-fits-all model that may over-protect or disempower capable minors.[62]
5. *Rigid divide between consent and contract.* The separation of data consent from contract law preserves doctrinal clarity but adds legal complexity, particularly in digital ecosystems where services involve both personal data processing based on consent and contractual obligations.[63]

Collectively, in its current form, Article 8 fails to provide a coherent, child-centred consent regime and must be reformed to reflect children's evolving capacities, technological realities and cross-border legal consistency. The next section analyses Article 8's shortcomings in detail.

3. Five Critical Fault-Lines

Article 8 of the GDPR suffers from at least five critical and interrelated weaknesses, which together undermine the GDPR's ability to provide consistent, effective and rights-based protection for children's personal data across the EU.

3.1 Legal Fragmentation: The Age Threshold Dilemma

This partial harmonisation caused by the below age limit between 13 and 16 years has resulted in a fragmented legal landscape, undermining the GDPR's goal of ensuring uniform protection and a consistent digital single market.[64] For example, the age of digital consent is set at 13 in Finland,[65] 14 in Spain and 16 in the Netherlands and Hungary.[66] As a result, a 14-year-old may provide valid consent in Spain but not in the Netherlands or Hungary, despite potentially having similar digital competence. Such inconsistencies complicate compliance for data controllers operating across borders. For instance, YouTube Kids, when processing kids' personal data such as IP addresses, search activity, location and device metadata, must determine whether parental consent is required based on the child's jurisdiction. The platform may need to seek parental consent for a 15-year-old in Hungary, but not in Spain.

This fragmented approach erodes the principle of equal treatment for children[67] across the EU and poses a direct challenge to the GDPR's harmonising ambition, especially for multinational ISS providers. Without a unified age threshold, the legitimacy of consent – and, by extension, the protection of children's personal data – remains uneven and legally uncertain.

[59] Verdoodt, "Safeguarding the Child's Right to Privacy"; Macenaite, "Consent for Processing Children's Personal Data."
[60] Regulation (EU) 2016/679; European Data Protection Board (EDPB), "Guidelines 8/2020 on the Targeting of Social Media Users."
[61] Kravchuk, "Privacy as a New Component"; Feldstein, "State Surveillance"; Land, "Sharenting"; Morehouse, "The Kids are Not Alright."
[62] Margaletić, "Children's Right to Privacy," 96.
[63] Kosta, "Article 8. Conditions Applicable to Child's Consent," 359.
[64] Macenaite, "Consent for Processing Children's Personal Data"; Caggiano, "Protecting Minors."
[65] Section 5, The Finnish Parliament, *Data Protection Act*, 2018.
[66] Macenaite, "Consent for Processing Children's Personal Data," 152–155.
[67] Article 2, United Nations, Convention on the Rights of the Child.

3.2 Ambiguity in Verifying Parental Consent: 'Reasonable Efforts' and 'Available Technology'

The lack of concrete legal norms surrounding the verification of parental consent through reasonable efforts, in the light of available technology, leaves the provision open to broad and subjective interpretation. This ambiguity has resulted in wide variations in practice across sectors and member states,[68] thereby undermining both legal certainty for controllers and consistent protection for children.

The principal difficulty lies in the absence of an EU-wide framework for determining parental authority. There is no unified European register identifying individuals with parental authority,[69] requiring controllers to rely on divergent national laws. These differences are substantial. For example, in Finland, married parents share custody by default, while unmarried mothers typically hold it unless otherwise ruled.[70] Moreover, in the United Kingdom (UK), married parents both have parental responsibility; unmarried fathers may obtain it via agreement or court order, and it can be shared among multiple individuals.[71] Luxembourg and Germany present similarly diverse frameworks that complicate consistent consent verification.[72] This diversity complicates the development of uniform consent-verification procedures, especially for cross-border services.

The lack of harmonisation also generates substantial compliance challenges for platforms operating across jurisdictions. The challenges are amplified in cross-border contexts, where conflicting national definitions of parental authority make standardised verification processes difficult to design and enforce. The 2022 fine imposed on Meta Ireland for failing to properly obtain parental consent for child users illustrates the practical and enforcement difficulties arising from interpretive and procedural uncertainty under Article 8(2).[73]

Further complexity arises from the undefined scope of 'available technology'. While the GDPR adopts a technology-neutral stance, as affirmed in Recital 15, the Regulation offers no concrete parameters for determining which technological tools are sufficient, proportionate and effective for verifying parental consent. The term 'available technology' can encompass a wide spectrum, from low-assurance measures such as email confirmations to higher-assurance methods including biometric checks, digital identity systems or government-issued eID verification.[74] Without authoritative guidance from the EDPB or the Court of Justice of the European Union (CJEU) on which methods meet the reasonable efforts standard in various risk contexts, controllers may adopt minimal or inconsistent safeguards. This not only increases compliance uncertainty, but may also expose children to heightened privacy risks where weak verification methods are used.[75]

Taken together, these definitional and procedural ambiguities dilute the effectiveness of Article 8(2), exposing children's personal data to inadequate protection and leaving controllers in legal limbo.

3.3 Too Many Responsibilities on the Holders of Parental Responsibility

The GDPR places significant reliance on parents or legal guardians to act in the best interests of the child when providing consent. The 'best interests' principle, enshrined in Article 3(1) of the UNCRC and Article 24(2) of the Charter, demands that all decisions by public[76] or private authorities affecting children must prioritise their welfare and rights.[77] In practice, however, this safeguard does not always operate effectively. One emerging challenge is the phenomenon commonly referred to as *sharenting*, whereby parents or guardians actively post and share children's personal information – such as images, birthdays, locations and hobbies – on social media platforms, often without considering the long-term implications.[78] This can lead to risks such as identity theft, data misuse and unauthorised surveillance.[79]

[68] Regulation (EU) 2016/679; European Data Protection Board (EDPB), "Guidelines 8/2020 on the Targeting of Social Media Users."
[69] Feiler, "Chapter II – Principles," 91.
[70] European Justice, "Parental Responsibility"; The Finnish Parliament, *Act on Child Custody and Right of Access*.
[71] The Parliament of the United Kingdom, *Children Act*.
[72] Switzerland – Association for Parental Responsibility, "Parental Responsibility"; Sections 1626–1698b, Federal Ministry of Justice, *Bürgerliches Gesetzbuch (BGB) – German Civil Code*.
[73] European Data Protection Board (EDPB), Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR.
[74] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679," 26.
[75] Kosta, "Article 8. Conditions Applicable to Child's Consent," 362.
[76] Court of Justice of the European Union, *Case C-61/22, RL v Landeshauptstadt Wiesbaden*, paras 93, 95.
[77] Official Journal of the European Union, Charter of Fundamental Rights of the European Union; United Nations Committee on the Rights of the Child, "General Comment No. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (Art 3, Para. 1)"; Court of Justice of the European Union, *Case C-61/22, RL v Landeshauptstadt Wiesbaden*.
[78] Land, "Sharenting."
[79] Kravchuk, "Privacy as a New Component"; Article 29 Data Protection Working Party, "Opinion on the Use of Location Data with a View to Providing Value-Added Services"; Livingstone, "Children."

Again, parents often provide consent under pressure or due to misinformation.[80] Parents may consent to digital services under pressure from children, societal norms or misleading marketing. For instance, educational platforms such as Google Classroom may require consent, but refusal could exclude the child from essential learning. In such cases, consent is neither fully informed nor freely given.[81]

Moreover, parents often consent to opaque data processing ecosystems, not understanding the complete data processing life-cycle.[82] In the context of Big Data (a technique of extensive collection and analysis of vast amounts of information, enabling insights and predictions),[83] personal data is often collected and processed in ways that cannot easily be foreseen by the data subject or the consenting parent. This undermines the meaningfulness of consent, particularly when parents are unaware of the extent of data tracking or downstream uses.[84]

Ultimately, while parental involvement remains essential,[85] their decisions do not always contribute to children's well-being. The GDPR lacks adequate safeguards to ensure that parental consent is both informed and aligned with the child's best interests.

3.4 Ethical Over-Reach and the Autonomy Paradox

The GDPR adopts a paternalistic model, assuming that children are not capable of providing informed consent below a certain age.[86] While this model aims to protect younger users, it fails to reflect the evolving capacities of older minors, particularly adolescents aged between 12 and 17 years.[87]

Research demonstrates that children develop privacy awareness earlier than the Regulation accounts for. Studies in the UK show that children as young as seven can discuss online risks, while those aged 11–18 express a desire for greater control over their personal data.[88] This growing digital literacy suggests that a blanket reliance on parental consent may suppress the agency of older minors, violating their rights to participation, informational self-determination and progressive involvement in decisions affecting them, principles affirmed in Articles 12, 13 and 16 of the UNCRC.

A more nuanced model is needed – one that tailors consent mechanisms to reflect a child's maturity and understanding, rather than a rigid age cutoff. Otherwise, the GDPR risks both over-protecting capable minors and under-protecting the most vulnerable by not supporting direct educational engagement about their data rights.

3.5 Legal Tensions Between Consent and Contractual Capacity

Article 8(3) preserves member states' autonomy over contract law, affirming that consent under Article 8 does not alter rules regarding minors' contractual capacity. While doctrinally sound, this separation creates practical confusion when services require both consent and a contractual agreement, especially for teenagers approaching adulthood.

For example, in Spain children aged 14 may provide digital consent,[89] but cannot enter into contracts independently until they are 18.[90] Thus, a child may lawfully consent to data processing but cannot engage in the terms of service. In the Netherlands, individuals below 18 are generally minors under the Civil Code,[91] but those aged 16 and above may enter into limited contracts with parental consent,[92] creating a potential mismatch: a minor may have contractual capacity but still require parental consent for data processing. Likewise, Hungary imposes one of the strictest dual layers, requiring parental consent for data processing below the age of 16[93] and restricting contractual capacity until 18, except for trivial daily purchases.[94] This may result in over-protection even for digitally competent teenagers.

[80] Feldstein, "State Surveillance," 2.
[81] Lindroos-Hovinheimo, "The Person in Control," 49.
[82] Solove, "Introduction," 1886.
[83] Cukier, "The Rise of Big Data," 30–33.
[84] Solove, "Introduction," 1881.
[85] Christakis, Handbook of Children and Screens, 373.
[86] Sehnalek, "Sharenting and Children's Privacy Protection," 130.
[87] Margaletić, "Children's Right to Privacy"; Bagattini, "Children's Well-Being"; Tobin, "Understanding Children's Rights: A Vision beyond Vulnerability."
[88] Bessant, "Children, Public Sector Data-Driven Decision-Making"; Dempsey, "Children Designing Privacy Warnings."
[89] Article 7, The Spanish Parliament, *Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights*.
[90] Articles 314, 315, 1263 The Spanish Parliament, *Spanish Civil Code*.
[91] Articles 233 and 234, The Dutch Parliament, *Dutch Civil Code Book 1*.
[92] Article 5, The Dutch Parliament, *General Data Protection Regulation Implementation Act*.
[93] Section 6(3), The Hungarian Parliament, *Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information*.
[94] Sections 2:8–2:12, The Hungarian Parliament, *Act V of 2013 on the Civil Code*.

In contrast, in Finland a child as young as 13 can consent under GDPR.[95] Finnish guardianship law and employment law recognise that minors (under 18) generally lack full contractual capacity,[96] but those aged 15 and above may independently make employment contracts and other legal agreements tied to their income.[97] The employment contract context may fall within the scope of Article 8 of the GDPR if the employment is conditioned on using a social media or messaging application platform such as Facebook or WhatsApp for communication purposes. This system risks under-protection if children engage in digital services without fully comprehending the privacy implications.

These legal discrepancies reveal a mismatch between data protection law and contract law, leading to inconsistent levels of autonomy and protection. The divergence complicates compliance for service providers and risks undermining the GDPR.

Together, these issues expose systemic vulnerabilities in Article 8's design and implementation, prompting the need for a reformed, harmonised and child-rights-based consent model, as the next section proposes.

4. Towards a Reformed Model of Child Consent under the GDPR

To effectively protect children's data protection rights in today's digital environment, Article 8 of the GDPR must be reformed into a harmonised, risk-sensitive and autonomy-respecting consent framework that better reflects children's evolving capacities[98] and legal inconsistencies across the EU.

4.1 Establishing a Harmonised Age Threshold for Digital Consent

A foundational step towards reform is the establishment of a uniform age of digital consent across all EU member states. The current regime's allowance for national derogations between 13 and 16 years has led to regulatory dissonance and unequal protection.[99] A harmonised age threshold would foster legal certainty for data controllers and ensure consistent safeguards for children across jurisdictions.

To achieve this, the EU could draw inspiration from regulatory models such as COPPA, which sets the digital consent age at under 13.[100] While COPPA has its limitations, it demonstrates that setting a uniform age for protecting children online is possible and feasible. A unified EU threshold—preferably set between 13 and 16—should be grounded in empirical assessments of cognitive development, digital literacy, and social expectations. Contextual flexibility may be preserved through narrowly tailored exceptions, such as supervised educational platforms or low-risk digital environments, provided additional safeguards are in place.

Such harmonisation would resolve existing cross-border inconsistencies, reduce administrative burdens, and strengthen the GDPR's objective of ensuring consistent child data protection within the digital single market.

4.2 Embedding a Risk-Calibrated Verification Framework for Parental Consent

To remedy the ambiguity in verifying parental consent, the GDPR should integrate a risk-tiered verification system that aligns the level of scrutiny with the nature and risk profile of the processing activity. Under this framework, the controller's obligation to verify parental consent would vary based on the severity of the potential impact on the child's rights and freedoms.[101] To illustrate, for low-risk processing – such as newsletter subscriptions or accessing non-personalised educational games – light verification methods, incorporating confirmation emails and declarations of parental responsibility, may suffice. Medium-risk scenarios – such as pseudonymised analytics or limited profiling – might require confirmation coupled with passive documentary evidence or digital signatures.

[95] Section 18, The Finnish Parliament, *Data Protection Act*, *2018.*
[96] Section 24, The Finnish Parliament, *Guardianship Service Act*; Section 3, The Finnish Parliament, *Employment Contracts Act*.
[97] Sections 2–3, The Finnish Parliament, *Young Workers' Act*.
[98] Morehouse, "The Kids Are Not Alright: A Look into the Absence of Laws Protecting Children in Social Media"; Nevická and Mesarčík, "Why Are You Offline? The Issue of Digital Consent and Discrimination of Roma Communities during Pandemic in Slovakia"; Bloomberg, "The Development and the Future of Privacy Law in Maine"; Livingstone, "Reframing Media Effects in Terms of Children's Rights in the Digital Age."
[99] Caggiano, "Protecting Minors as Technologically Vulnerable Persons through Data Protection: An Analysis on the Effectiveness of Law," 27.
[100] Macenaite, "Consent for Processing Children's Personal Data," 168.
[101] Kosta, "Article 8. Conditions Applicable to Child's Consent," 361.

Conversely, high-risk contexts – such as behavioural profiling, biometric tracking or data-intensive social media use[102] – demand robust verification tools. These may include identity document uploads, proof of parental relationship like birth certificates or use of national digital identity systems compliant with the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation.[103] eIDAS is an EU regulation[104] that establishes standards for electronic identification and trust services, ensuring secure, cross-border digital transactions and electronic signatures across EU member states for individuals, businesses and public administrations. Controllers operating in countries such as Estonia, Belgium and Germany can already leverage such systems.[105]

Importantly, this model must align with the GDPR's data-minimisation principle, ensuring that verification processes do not themselves infringe on data protection rights.[106] Verification should be proportionate, avoiding over-collection while ensuring that the identity and authority of the consenting individual are adequately established.

Given the GDPR's technology-neutral stance,[107] the proposed framework would not mandate specific tools but instead require context-based justification for the selected method. This aligns with the EDPB guidance, which advocates for tailoring safeguards to the sensitivity and scale of data processing.[108]

4.3 Making Parental Consent More Informed, Transparent and Responsible

While parental involvement is vital, its effectiveness depends on informed, voluntary and context-sensitive decision-making. Enhancing parental consent mechanisms under the GDPR requires strengthening transparency obligations, improving digital literacy and addressing the structural imbalances that can compromise the voluntariness of consent.

First, controllers must provide clear, accessible and age-appropriate privacy notices that explain the categories of personal data collected, the purposes of processing[109] and the associated risks.[110] This requirement is rooted in the GDPR's transparency requirements (Articles 5(1), 12, 13 and 14) and has been reinforced through enforcement actions. For example, the Dutch Data Protection Authority (DPA) fined TikTok for failing to provide clear privacy information to Dutch children.[111] Again, in 2023, the Irish DPA imposed a €345 million fine on TikTok for not providing clear and accessible information to children about default public settings.[112] Notably, the Irish decision also examined whether the collection and use of children's data was 'fair' under Article 5(1)(a) GDPR,[113] signalling that EU supervisory authorities may scrutinise processing beyond the consent paradigm. While the focus of this article remains on consent obligations, such enforcement underscores the broader baseline protections – such as fairness, lawfulness and purpose limitation[114] – that operate alongside consent in protecting children's data.

Second, strengthening parental decision-making requires targeted digital literacy initiatives at both the national and EU levels. These programs should educate parents and guardians about surveillance capitalism, targeted advertising and the long-term consequences of data sharing. The UNCRC[115] and most EU countries, including Finland, already provide statutory frameworks on the duties of guardians;[116] these could serve as a normative foundation for embedding children's data-protection awareness into everyday parenting practices.

Third, voluntariness in consent is undermined when it is sought in contexts of significant power imbalance. The GDPR explicitly warns against using consent as a lawful basis in such circumstances, as in the case of the Skellefteå municipality in Sweden. The Swedish DPA fined the municipality for using facial recognition technology to monitor school attendance with

[102] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679," WP 248 rev:9–10.
[103] Obserwatorium biz, "EIDAS 2.0 in Europe."
[104] Regulation (EU) No 910/2014.
[105] Obserwatorium biz, "EIDAS 2.0 in Europe."
[106] Piasecki, "Complying with the GDPR," 124.
[107] Recital 15, Regulation (EU) 2016/679.
[108] European Data Protection Board (EDPB), "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default," 9.
[109] Faisal, "Applying the Purpose Limitation Principle," 67.
[110] Article 12(1), Regulation (EU) 2016/679.
[111] Dutch DPA, "TikTok Fined."
[112] Irish Data Protection Commission, "Irish Data Protection Commission Announces €345 Million Fine."
[113] Irish Data Protection Commission, "Irish Data Protection Commission Announces €345 Million Fine."
[114] Malgieri, Vulnerability and Data Protection Law, 234; Faisal, "Book Review: Gianclaudio Malgieri," 103.
[115] Articles 5 and 18, United Nations, Convention on the Rights of the Child.
[116] Chapter 5, The Finnish Parliament, *Guardianship Service Act*.

parental consent,[117] which was deemed invalid because the relationship between the school and parents was inherently imbalanced, limiting the possibility of freely given consent.[118] In digital environments, 'dominant platforms' such as large social media networks or app ecosystems may exercise similar structural leverage over users, making both child and parental consent suspect when there is no genuine ability to refuse without significant loss of access or utility. In such scenarios, reliance on alternative lawful bases – such as performance of a task carried out in the public interest, compliance with a legal obligation or legitimate interests (subject to Article 6(1) and Article 6(4) balancing tests) – may be more appropriate.[119] This reflects the broader critique in privacy scholarship that consent mechanisms often over-estimate individual capacity to manage privacy in environments characterised by information asymmetries and constrained choices.[120]

Finally, a sustainable model of children's data governance requires moving beyond over-reliance on parental control towards recognising children's evolving capacities and gradual autonomy. Parental authority should be exercised in the best interests of the child, not as a blanket veto in line with Article 12 of the UNCRC. Children's voices must be meaningfully involved in decisions affecting their privacy, with their views given due weight according to their age and maturity.[121] This shift recognises that protecting children's data requires not only stronger consent mechanisms, but also embedding fairness, transparency and respect for children's agency into the design of digital services.

4.4 Recognising and Operationalising Evolving Capacity in Consent

The GDPR could better reflect the principle of children's evolving capacities that account for their developing cognitive skills, maturity and ability to make informed decisions in digital spaces. A revised consent framework should explicitly recognise that many adolescents – particularly older minors – possess the maturity and contextual understanding necessary to exercise meaningful data rights. Research across domains,[122] including medical research,[123] demonstrates that minors can demonstrate resilience, self-agency and the capacity to collaborate effectively with adults in decision-making processes when appropriately supported.[124]

One potential reference point is the *Gillick* competence test,[125] developed in UK jurisprudence, which permits minors to make certain decisions independently if they demonstrate a sufficient understanding of the nature, purpose and consequences of the decision.[126] Applied to the data-protection context, such an approach would allow competent adolescents to provide valid consent without parental authorisation, particularly where the processing relates to services that they routinely use and can meaningfully understand. This would complement rather than replace a harmonised EU age threshold for parental consent under Article 8(1) GDPR. A uniform threshold would establish a baseline presumption of when parental involvement is required, while the *Gillick*-style individual assessment could function as a flexible exception, appropriate in circumstances where the adolescent's competence is demonstrable and the nature of the processing is neither high-risk nor beyond their capacity to evaluate. This dual model would preserve legal certainty while accommodating the diversity of children's developmental trajectories.

The normative foundation for such an evolution-based model is grounded in the UNCRC. Article 5 recognises children's growing capacity to make decisions in line with their development, while Article 12 emphasises their right to be heard in all matters affecting them.[127] Integrating these principles into GDPR implementation would ensure that digital consent mechanisms reflect both developmental psychology and fundamental rights law.

[117] BBC News, "Facial Recognition."
[118] European Data Protection Board (EDPB), "Facial Recognition in School"; Quintel, "Sweden."
[119] Verdoodt, "Safeguarding the Child's Right to Privacy," 130.
[120] Solove, "Introduction," 1903.
[121] European Commission, Artificial Intelligence and the Rights of the Child, 67.
[122] Tobin, "Understanding Children's Rights," 178.
[123] Taylor, "When Can the Child Speak for Herself?," 369.
[124] Christakis, Handbook of Children and Screens, 207.
[125] The *Gillick* test, established by the House of Lords in 1985 in the case *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] AC 112, determines whether a child under 16 can consent to medical treatment without parental knowledge or approval. It originated in England and Wales, and is based on whether the child has sufficient maturity and understanding to make informed decisions. The test is legally binding in England and Wales and has influenced legal standards in Australia, Canada and New Zealand.
[126] Taylor, "When Can the Child Speak for Herself?," 370.
[127] United Nations Committee on the Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," para 71.

Operationalising evolving capacity in practice would require tools that promote comprehension and meaningful engagement. These could include interactive, age-adapted disclosures;[128] consent dashboards enabling children to review and adjust permissions over time; educational interfaces explaining data uses in accessible language;[129] and comprehension-based prompts designed to test understanding before consent is finalised. Such tools can simultaneously assist parents in making more informed choices, thereby bridging the information gap that currently undermines consent validity.

Embedding these participatory mechanisms into digital ecosystems would shift the regulatory focus from merely protecting children from harm to actively fostering their agency, digital citizenship and informed decision-making. In doing so, the GDPR would better align with its dual commitment to safeguarding children's rights and enabling their active participation in the digital society.

4.5 Towards a Capacity-Based and Harmonised Consent Framework

The fragmentation created by varying national contract laws and differing interpretations of consent capacity poses one of the most significant structural challenges to consistent child data protection in the EU. To remedy this, a two-pronged strategy is proposed.

First, the EDPB should issue binding guidance under Article 70 of the GDPR, clarifying the interaction between digital consent and national rules on contractual capacity. This guidance should provide interpretive tools to assess a child's competence to give informed, specific and voluntary consent, independent of their contractual status under the Civil Laws.

Second, the GDPR could be amended or supplemented to establish a minimum EU-wide digital consent age, while allowing member states to retain their domestic rules on contracts. This distinction would respect subsidiarity while promoting coherence in data protection.

To further enhance this framework, the development and implementation of Child Rights Impact Assessments (CRIAs) should be encouraged. These assessments, grounded in Articles 4 and 12 of the UNCRC,[130] evaluate how data processing affects children's rights, including privacy, participation, freedom of expression and well-being. They provide a structured method for integrating child-centric considerations into digital service design and decision-making.

CRIAs should be mandatory in high-risk data processing contexts involving children's personal data. This includes activities such as profiling, predictive analytics, targeted marketing, monitoring, large-scale data processing and matching or combining datasets.[131] CRIAs should also be required when new technologies are used to process children's personal data.[132] These assessments should complement the Data Protection Impact Assessment (DPIA) required under Article 35 of the GDPR, which systematically evaluates risks to the rights and freedoms of data subjects. While the DPIA focuses on data-protection risks to human rights and freedoms in general, the CRIA provides an added framework that centres on child rights and welfare. Controllers are encouraged to adopt CRIAs more broadly through codes of conduct (Article 40 GDPR) and sectoral guidelines under the GDPR. These tools promote a principled and proactive approach to aligning data-protection practices with the best interests of the child, thereby supporting rights-based innovation.

Overall, a reformed consent model must empower children as active digital rights-holders, not just passive objects,[133] and calls for systemic legal, procedural and educational reforms to realise this vision. The next section explores the broader implications of this reformed model.

5. Discussion

This article has examined the deficiencies of the GDPR's current consent framework for processing children's personal data and advanced a reform proposal rooted in harmonisation, risk sensitivity and recognition of evolving capacity. The discussion

[128] Christakis, Handbook of Children and Screens, 472.
[129] Christakis, Handbook of Children and Screens, 539.
[130] United Nations Committee on the Rights of the Child, "General Comment No 5 on General Measures of Implementation of the Convention on the Rights of the Child (Arts 4, 42 and 44, Para. 6)," para 45.
[131] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679," WP 248 rev:9–10.
[132] Article 29 Data Protection Working Party, WP 248 rev:9–10.
[133] Carey, "Some Ethical Limitations," 272.

now turns to the broader implications of these findings, reflecting on their legal, ethical and regulatory significance within the evolving digital ecosystem.

A central theme emerging from this study is the tension between child protection and child empowerment. The GDPR's consent mechanism, as it is currently framed, prioritises protective paternalism – largely through parental control – without sufficiently accommodating the growing digital competence of children, particularly adolescents. While protection remains essential, particularly for younger or vulnerable children, the legal framework must adapt to acknowledge children not only as subjects in need of safeguarding but as rights-holders capable of engaging with data-governance processes.[134] This calls for a normative shift from a child-as-object[135] paradigm to a child-as-agent model,[136] consistent with both the UNCRC and contemporary understandings of children's digital citizenship.

From a legal standpoint, two structural weaknesses stand out: the fragmented age of digital consent across member states and the indeterminacy surrounding verification obligations for parental consent. These inconsistencies impose disproportionate burdens on data controllers operating across borders. The current model, by permitting member states to deviate on such a foundational concept, effectively creates a patchwork of regulatory standards, contrary to the spirit of a unified digital single market.

The proposed reform model – anchored in uniform consent thresholds, risk-calibrated verification and age-appropriate transparency – offers a viable path to restore coherence and legal certainty. Importantly, this model maintains the GDPR's principle of proportionality,[137] while better aligning legal obligations with technological realities and social practices. A risk-based consent verification mechanism, for instance, does not impose blanket obligations but adjusts the rigor of verification to the potential impact of processing activities. This approach not only supports practical feasibility, but also ensures that children in high-risk contexts are not left unprotected due to vague standards or enforcement disparities.

Ethically, the principles of dignity,[138] autonomy and justice are central to the consent process.[139] Consent, as a manifestation of individual autonomy, must be meaningful, requiring that data subjects understand what they agree to and that they are free to withhold or withdraw that agreement. In the context of children – especially adolescents – these ethical obligations cannot be sidelined. Children's lived digital experiences are often sophisticated, and many demonstrate nuanced awareness of online risks. Denying them the opportunity to participate in such decisions risks undermining their agency and rights.

Embedding children's voices into digital policy and data governance is essential. Tools such as CRIAs and participatory consent interfaces offer promising avenues for institutionalising such engagement. These mechanisms would not only elevate children's perspectives in design and policy-making but also foster a culture of rights-based digital development,[140] where consent is understood as a dynamic process rather than a one-time procedural hurdle.

From a regulatory standpoint, the proposed reforms demand stronger coordination between EU institutions and national authorities. The EDPB, in particular, has a pivotal role in issuing interpretive guidance that bridges national divergences, especially in reconciling consent and contract laws. The development of sector-specific codes of conduct, as encouraged under Article 40 of the GDPR, could further standardise best practices and support implementation across varied platforms and services.

However, the law alone cannot resolve all dimensions of children's digital vulnerability.[141] Business models predicated on surveillance-based monetisation,[142] technological design patterns that exploit behavioral biases[143] and broader socio-economic structures contribute significantly to the risks faced by children online. Addressing these requires a multi-pronged strategy that integrates legal reform with ethical design practices, digital literacy initiatives, transparency-enhancing technologies and

[134] Tobin, "Understanding Children's Rights," 158.
[135] Carey, "Some Ethical Limitations," 283.
[136] Macleod, "Paradoxes of Children's Vulnerability," 267.
[137] Faisal, "Navigating the Fine Line," 7.
[138] Kravchuk, "Privacy as a New Component"; Court of Justice of the European Union, Case C-61/22, *RL v Landeshauptstadt Wiesbaden.*
[139] United Nations Committee on the Rights of the Child, "General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment," 11–13.
[140] Livingstone, "Reframing Media Effects."
[141] Faisal, "Decoding Vulnerability."
[142] Article 29 Data Protection Working Party, "Opinion on the Use of Location Data with a View to Providing Value-Added Services," 8–9.
[143] European Commission, Artificial Intelligence and the Rights of the Child, 76.

institutional accountability mechanisms. Strengthening parental understanding of digital risks, while simultaneously cultivating children's data literacy and participatory skills, will be central to the long-term effectiveness of the reform.

In summary, this discussion underscores the need for a principled, adaptive and child-centred approach to consent under the GDPR. The pathway to reform must be collaborative, engaging regulators, educators, technologists, parents and children themselves to ensure that digital environments become not only safer but also more inclusive, respectful and empowering for all young users.

Finally, the study is not without its limitations. It relies primarily on legal analysis and secondary sources, which may overlook empirical insights into children's and parents' lived experiences with digital consent. The rapidly evolving technological landscape also poses challenges for fully anticipating future verification methods and privacy risks. Additionally, while focusing on the GDPR and EU context, the study offers limited comparative analysis of non-European regulatory frameworks beyond brief references, potentially constraining the generalisability of recommendations.

6. Conclusion

This study reveals that Article 8 of the GDPR, in its current form, falls short of delivering consistent, clear and rights-based protection to children's personal data across the EU. Fragmented age thresholds, ambiguous consent verification standards, over-reliance on parental authority, inadequate recognition of children's evolving capacity and misalignment with contractual capacity laws all create legal uncertainty, uneven safeguards and barriers to children's meaningful participation in data governance. There is an urgent need to reform the GDPR's child consent framework to better protect children's personal data. A harmonised, risk-sensitive and autonomy-aware consent model, supported by clear regulatory guidance, participatory mechanisms and coordinated enforcement, offers a viable path forward. Yet legal reform alone is insufficient; sustained impact will require integrating ethical design, digital literacy, and accountability measures into the broader digital ecosystem. Aligning protection with empowerment is essential to ensuring that children's digital environments are not only safer but also more inclusive, respectful and responsive to their evolving capacities.

Future research should empirically examine how children and parents experience digital consent mechanisms across diverse contexts to inform practical implementation. Additionally, exploring the integration of emerging technologies, such as Artificial Intelligence (AI)-driven verification tools, could provide valuable insights into balancing privacy protection with usability. These directions will be critical for ensuring that legal frameworks remain adaptive and effective in safeguarding children's rights in an evolving digital environment.

Funding
This research was supported by the Generation AI Project at the University of Helsinki, funded by the Strategic Research Council (STN) through the Academy of Finland (Contract No. 01331393).

Acknowledgements
The author thanks the anonymous reviewers for their insightful comments and constructive suggestions, which have significantly improved the quality of this article. The author also gratefully acknowledges the support of the in-house language revision services for their meticulous editorial assistance.

Bibliography

Article 29 Data Protection Working Party. "Guidelines on Consent under Regulation 2016/679," (2018).

Article 29 Data Protection Working Party. "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679." *Article 29 Working Party*. Vol. WP 248 rev (2017).

Article 29 Data Protection Working Party. "Opinion on the Use of Location Data with a View to Providing Value-Added Services" (2005).

Bagattini, Alexander. "Children's Well-Being and Vulnerability." *Ethics and Social Welfare* 13, no 3 (2019): 211–215. https://doi.org/10.1080/17496535.2019.1647973.

BBC News. "Facial Recognition: School ID Checks Lead to GDPR Fine", August 28, 2019. https://www.bbc.com/news/technology-49489154.

BBC News. "YouTube Fined $170m in US Over Children's Privacy Violation." *BBC*, September 5, 2019. https://www.bbc.com/news/technology-49578971.

Bessant, Claire. "Children, Public Sector Data-Driven Decision-Making and Article 12 UNCRC." *European Journal of Law and Technology* 13, no 2 (2022): 1–33. https://ejlt.org/index.php/ejlt/article/download/872/1056.

Bloomberg, Scott. "The Development and the Future of Privacy Law in Maine." *Maine Law Review* 73, no 2 (2021): 215–70. https://illinoisjltp.com/file/244/Brunngraber_2024_Issue%201.pdf.

Caggiano, Ilaria Amelia. "Protecting Minors as Technologically Vulnerable Persons Through Data Protection: An Analysis on the Effectiveness of Law." *European Journal of Privacy Law & Technologies* 1 (2022): 27–44. https://doi.org/10.57230/ejplt221iac.

Carey, Malcolm. "Some Ethical Limitations of Privatising and Marketizing Social Care and Social Work Provision in England for Children and Young People." *Ethics and Social Welfare* 13, no 3 (2019): 272–87. https://doi.org/10.1080/17496535.2019.1585466.

Christakis, Dimitri A and Lauren Hale. *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence*. Cham: Springer, 2025.

Council of Europe. *European Convention on Human Rights*. Brussels: Council of Europe, 1950.

Court of Justice of the European Union. Case 263/86, *Belgian State and René Humbel and Marie-Thérèse Humbel, née Edel* (1988).

Court of Justice of the European Union. Case 352/85, *Bond van Averteerders and Others and The Netherlands State* (1988).

Court of Justice of the European Union. Case C-34/21, *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums*, ECLI:EU:C:2023:270 (2023).

Court of Justice of the European Union. Case C-61/22, *RL v Landeshauptstadt Wiesbaden*, ECLI:EU:C:2024:251 (2024).

Court of Justice of the European Union. Opinion of Advocate General Pitruzzella delivered on 27 January 20221 Case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:65 (2022).

Cukier, Kenneth Neil and Viktor Mayer-Schoenberger. "The Rise of Big Data: How It's Changing the Way We Think About the World." *Foreign Affairs* 92, no 3 (2013): 28–40. https://www.jstor.org/stable/23526834.

Dempsey, John, Gavin Sim, Brendan Cassidy and Vinh-Thong Ta. "Children Designing Privacy Warnings: Informing a Set of Design Guidelines." *International Journal of Child–Computer Interaction* 31 (2022): 1–18. https://doi.org/10.1016/j.ijcci.2021.100446.

Dethloff, Nina. "Families and the Law: Taking Account of Children's Evolving Capacities in Analogue and Digital Contexts." In *Families and New Media: Comparative Perspectives on Digital Transformations in Law and Society*, edited by Nina Dethloff, Katharina Kaesling and Louisa Specht-Riemenschneider, 102–20. Wiesbaden: Springer, 2013.

Digital Futures Commission. *Governance of Data for Children's Learning in UK State Schools.* London: Digital Futures Commission, 2021.

Dutch DPA. "TikTok Fined for Violating Children's Privacy." European Data Protection Board, 2021. https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en.

The Dutch Parliament. *Dutch Civil Code Book 1* (1838). https://wetten.overheid.nl/BWBR0002656/2019-01-29/#Boek1_Titeldeel14_Afdeling6_Paragraaf4_Artikel302.

The Dutch Parliament. *General Data Protection Regulation Implementation Act* (2018). https://wetten.overheid.nl/BWBR0040940/2021-07-01.

European Commission. *Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy.* Brussels: European Union, 2022.

European Data Protection Board (EDPB). Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR (2022).

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

European Data Protection Board (EDPB). "Facial Recognition in School Renders Sweden's First GDPR Fine." 2019. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv.
European Data Protection Board (EDPB). "Guidelines 05/2020 on Consent under Regulation 2016/679." 2020.
European Data Protection Board (EDPB). "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default." 2020. https://doi.org/10.21552/edpl/2020/4/14.
European Data Protection Board (EDPB). "Guidelines 8/2020 on the Targeting of Social Media Users." 2020.
European Data Protection Supervisor. Data Protection (2021). https://edps.europa.eu/data-protection/data-protection_en.
European Justice. "Parental Responsibility - Child Custody and Contact Rights." 2024. https://e-justice.europa.eu/topics/family-matters-inheritance/parental-responsibility-child-custody-and-contact-rights/fi_en?utm_source=chatgpt.com.
European Parliament. "Children's Rights in the EU in the Light of the UN Convention on the Rights of the Child." 2022. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)738223.
European Union. Consolidated version of the Treaty on the Functioning of the European Union, Pub. L. No. 2008/C 115/01, 47 (2007). https://doi.org/10.1080/03235408.2013.817161.
European Union. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), L 241 Official Journal of the European Union § (2015). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&from=EN.
European Union Agency for Fundamental Rights. "Consent to Use Data on Children." https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consent-use-data-children.
Faisal, Kamrul. "Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective." *Communication Law and Policy* 28, no 1 (2023): 67–97. https://doi.org/10.1080/10811680.2023.2180266.
Faisal, Kamrul. "Book Review: Gianclaudio Malgieri, *Vulnerability and Data Protection Law*. Oxford University Press, 2023." *Tidskrift Utgiven Av Juridiska Föreningen i Finland*, nos 1–2 (2024): 99–109. https://www.edilex.fi/jft/1001150004.
Faisal, Kamrul. "Children's Rights to Personal Data Protection: Why the GDPR Falls Short." *EU Law Live Weekend Edition*, 223 (2025): 1–10. https://helda.helsinki.fi/server/api/core/bitstreams/9659e04c-e63b-436f-8b91-eda2a34be382/content.
Faisal, Kamrul. "Decoding Vulnerability Within the GDPR." CiTiP Blog, 2024. https://www.law.kuleuven.be/citip/blog/decoding-vulnerability-within-the-gdpr.
Faisal, Kamrul. "Navigating the Fine Line: The Complex Reconciliation of Data Protection and Freedom of Expression in Criminal Conviction and Offences Data." *Digital Policy, Regulation and Governance*, 1–18. https://doi.org/10.1108/DPRG-10-2024-0260.
Federal Ministry of Justice. Bürgerliches Gesetzbuch (BGB) – German Civil Code (2002). https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.pdf.
Federal Trade Commission. "Complying with COPPA: Frequently Asked Questions." 2020. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#D.
Feiler, Lukas, Forgó Nikolaus, and Michaela Weigl. "Chapter II – Principles." In *The EU General Data Protection Regulation (GDPR): A Commentary*, 74–105. Woking: Globe Law and Business, 2018.
Feldstein, Steven. "State Surveillance and Implications for Children." New York: UNICEF, 2020. https://www.unicef.org/innocenti/media/1136/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf.
The Finnish Parliament. Act on Child Custody and Right of Access, Pub. L. No. 361/1983 (1983). https://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_10/spl_78/pdfs/39.pdf.
The Finnish Parliament. Data Protection Act, Pub. L. No. 1050/ 2018, 2 Ministry of Justice, Finland 227-249 (2018).
The Finnish Parliament. Data Protection Act, Pub. L. No. 1050/2018, 1 (2018). https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.
The Finnish Parliament. Employment Contracts Act, Pub. L. No. 55/2001 (2011). https://finlex.fi/api/media/statute-foreign-language-translation/220146/mainPdf/main.pdf?timestamp=2001-01-26T00%3A00%3A00.000Z.
The Finnish Parliament. Guardianship Service Act, Pub. L. No. 442/1999, 1 (1999). https://finlex.fi/api/media/statute-foreign-language-translation/235368/mainPdf/main.pdf?timestamp=1999-04-01T00%3A00%3A00.000Z.
The Finnish Parliament. Young Workers' Act, Pub. L. No. 998/1993, 1 (1993). https://finlex.fi/api/media/statute-foreign-language-translation/296896/mainPdf/main.pdf?timestamp=1993-11-19T00%3A00%3A00.000Z.
Fosch-Villaronga, Eduard, Simone van der Hof, Christoph Lutz and Aurelia Tamò-Larrieux. "Toy Story or Children Story? Putting Children and Their Rights at the Forefront of the Artificial Intelligence Revolution." *AI and Society* 38, no 1 (2023): 133–152. https://doi.org/10.1007/s00146-021-01295-w.

Gonçalves, Maria Eduarda. "The Risk-Based Approach under the New EU Data Protection Regulation: A Critical Perspective." *Journal of Risk Research* 23, no. 2 (2020): 139–152. https://doi.org/10.1080/13669877.2018.1517381.
The Hungarian Parliament. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (2011). https://www.naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf.
The Hungarian Parliament. Act V of 2013 on the Civil Code (2013). https://faolex.fao.org/docs/pdf/hun209514.pdf.
Hutchinson, Terry. "Doctrinal Research: Researching the Jury." In *Research Methods in Law*, edited by Dawn Watkins and Mandy Burton, 8–39. London: Routledge, 2018.
Irish Data Protection Commission. "Irish Data Protection Commission Announces €345 Million Fine of TikTok." Dublin: Irish Data Protection Commission, 2023. https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok.
Kosta, Eleni. "Article 7. Conditions for Consent." In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A Bygrave and Christopher Docksey, 345–354. Oxford: Oxford University Press, 2020.
Kosta, Eleni. "Article 8. Conditions Applicable to Child's Consent in Relation to Information Society Services." In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A Bygrave and Christopher Docksey, 355–364. Oxford: Oxford University Press, 2020.
Kravchuk, Natasha. "Privacy as a New Component of 'The Best Interests of the Child' in the New Digital Environment." *The International Journal of Children's Rights* 29 (2021): 99–121. https://doi.org/10.1163/15718182-29010006.
Land, Kate. "Sharenting: Do You Share Too Much About Your Children on Social Media?" *US News Health*, February 13, 2017. https://health.usnews.com/wellness/for-parents/articles/2017-02-13/sharenting-do-you-share-too-much-about-your-children-on-social-media.
Lindroos-Hovinheimo, Susanna. "The Person in Control." In *Private Selves: Legal Personhood in European Privacy Protection*, 44–68. Cambridge: Cambridge University Press, 2021.
Livingstone, Sonia. "Children: A Special Case for Privacy?" *Intermedia* 46, no 2 (2018): 18–23. http://eprints.lse.ac.uk/89706/1/Livingstone_Children-a-special-case-for-privacy_Published.pdf.
Livingstone, Sonia. "Reframing Media Effects in Terms of Children's Rights in the Digital Age." *Journal of Children and Media* 10, no 1 (2016): 4–12. https://doi.org/10.1080/17482798.2015.1123164.
Livingstone, Sonia and Kim R. Sylwander. "Conceptualizing Age-Appropriate Social Media to Support Children's Digital Futures." *British Journal of Developmental Psychology*, April (2025): 1–13. https://doi.org/10.1111/bjdp.70006.
Macenaite, Milda and Eleni Kosta. "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?" *Information and Communications Technology Law* 26, no 2 (2017): 146–197. https://doi.org/10.1080/13600834.2017.1321096.
Macleod, Colin. "Paradoxes of Children's Vulnerability." *Ethics and Social Welfare* 13, no 3 (2019): 261–271. https://doi.org/10.1080/17496535.2019.1630465.
Malgieri, Gianclaudio. "In/Acceptable Marketing and Consumers' Privacy Expectations: Four Tests from EU Data Protection Law." *Journal of Consumer Marketing* 40, no 2 (2023): 209–223. https://doi.org/10.1108/JCM-03-2021-4571.
Malgieri, Gianclaudio. *Vulnerability and Data Protection Law*. Edited by Christopher Kuner and Graham Greenleaf. Oxford: Oxford University Press, 2023.
Malgieri, Gianclaudio and Gloria González Fuster. "The Vulnerable Data Subject: A Gendered Data Subject?" *European Journal of Law and Technology* 13, no 2 (2022): 1–26. https://doi.org/10.2139/ssrn.3913249.
Malgieri, Gianclaudio and Jędrzej Niklas. "Vulnerable Data Subjects." *Computer Law and Security Review* 37, no 788039 (2020): 1–16. https://doi.org/10.1016/j.clsr.2020.105415.
Margaletić, Anica Čulo and Barbara Preložnjak. "Children's Right to Privacy in the Digital Age." *Intereulaweast* 10, no 2 (2023): 81–100. https://doi.org/10.22598/iele.2023.10.2.4.
Morehouse, Libby. "The Kids are Not Alright: A Look into the Absence of Laws Protecting Children in Social Media." *Loyola of Los Angeles Entertainment Law Review* 44, no 2 (2024): 75–127. https://digitalcommons.lmu.edu/elr/vol44/iss2/2.
Nevická, Denisa and Matúš Mesarčík. "Why are You Offline? The Issue of Digital Consent and Discrimination of Roma Communities During Pandemic in Slovakia." *International Journal of Discrimination and the Law* 22, no 2 (2022): 172–191. https://doi.org/10.1177/13582291221096615.
Obserwatorium biz. "EIDAS 2.0 in Europe: Implementation and Use Cases." 2024. https://obserwatorium.biz/en/eidas-2-0-w-europie-implementacja-i-przypadki-uzycia.html.
Official Journal of the European Union. Charter of Fundamental Rights of the European Union, Pub. L. No. (2016/C 202/02), 389-405 (2016). https://doi.org/10.4337/9781786435477.00032.
Official Journal of the European Union. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Pub. L. No. L 257, 73 (2014).

Oostveen, Manon, Kristina Irion, Helena Ursic, Philipp Hacker, Inge Graef, Anca D. Chirita, Björn Lundqvist et al. *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Berlin: Springer-Verlag, 2018. https://link.springer.com/content/pdf/10.1007/978-3-662-57646-5.pdf.

The Parliament of the United Kingdom. *Children Act*, Pub. L. No. c. 41, 1 (1989). https://www.legislation.gov.uk/ukpga/1989/41/data.pdf.

Piasecki, Stanislaw and Jiahong Chen. "Complying with the GDPR When Vulnerable People Use Smart Devices." *International Data Privacy Law* 12, no 2 (2022): 113–131. https://doi.org/10.1093/idpl/ipac001.

Quintel, Teresa. "Sweden: The First GDPR Fine in the Country of Openness: Is Sweden Moving Towards More Privacy?" *European Data Protection Law Review* 5, no. 4 (2019): 548–553. https://doi.org/10.21552/edpl/2019/4/15.

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) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.

Sehnalek, David. "Sharenting and Children's Privacy Protection in International, EU, and Czech Law: Parents, Stop Sharing! Thank You, Your Children." *Central European Journal of Comparative Law* 4, no 1 (2023): 111–32. https://doi.org/10.47078/2023.1.111-132.

Solove, Daniel J. "Introduction: Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126, no 7 (2013): 1880–1903. https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma.

The Spanish Parliament. Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights, Pub. L. No. 16673 (2018). https://www.uspceu.com/Portals/0/docs/transparencia/normativa/legislacion-general/EN - Organic Law 3-2018, of December 5, on Personal Data Protection and guarantee of digital rights.pdf.

The Spanish Parliament. Spanish Civil Code, Pub. L. No. 051-16-022–9, 1 (2016).

Switzerland – Association for Parental Responsibility. "Parental Responsibility: The Luxembourg Model in Detail," 2023. https://vev.ch/en/parental-responsibility-the-luxembourg-model-in-detail.

Taylor, Mark J., Edward S. Dove, Graeme Laurie and David Townend. "When Can the Child Speak for Herself? The Limits of Parental Consent in Data Protection Law for Health Research." *Medical Law Review* 26, no 3 (2018): 369–391. https://doi.org/10.1093/MEDLAW/FWX052.

Thompson, Clive. "How Videogames Like Minecraft Actually Help Kids Learn to Read." *Wired*, October 2014. https://www.wired.com/2014/10/video-game-literacy.

Tobin, John. "Understanding Children's Rights: A Vision Beyond Vulnerability." *Nordic Journal of International Law* 84, no 2 (2015): 155–182. https://doi.org/10.1163/15718107-08402002.

US Congress. *Children's Online Privacy Protection Act* 15 USC §§ 6501–6506 (1998).

United Nations. *Convention on the Rights of the Child* (1989). https://doi.org/10.1111/j.1467-9515.1989.tb00500.x.

United Nations Committee on the Rights of the Child. "General Comment No. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (Art. 3, Para. 1)." Vol. CRC/C/GC/1, 2013.

United Nations Committee on the Rights of the Child. "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment." Vol. CRC/C/GC/2, 2021. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjH1P_fzPODAxUZQVUIHfHkC68QFnoECBEQAQ&url=https%3A%2F%2Fdocstore.ohchr.org%2FSelfServices%2FFilesHandler.ashx%3Fenc%3D6QkG1d%252FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%252F5F0.

United Nations Committee on the Rights of the Child. "General Comment No. 5 on General Measures of Implementation of the Convention on the Rights of the Child (Arts. 4, 42 and 44, Para. 6)." Vol. CRC/GC/200, 2003. https://www.refworld.org/legal/general/crc/2003/en/36435.

Verdoodt, Valerie, Yueming Zhang and Eva Lievens. "Safeguarding the Child's Right to Privacy and Data Protection in the European Union and China: A Tale of State Duties and Business Responsibilities." *The International Journal of Human Rights* 28, no 2 (2024): 125–147. https://doi.org/10.1080/13642987.2023.2233917.

Zampino, Letizia. "Book Review: Deborah Lupton *The Quantified Self. A Sociology of Self-Tracking*. Cambridge: Polity Press, 2016." *Tecnoscienza* 9, no 1 (2018): 139–142.