

UGANDA: UNDERSTANDING CHILDREN'S DATA PRIVACY RIGHTS



Lawpoint Uganda
Making the Law Easy and Accessible

Partner



DPO
PRIVACY CENTRE
EAST AFRICA

Introduction

The right to privacy is a fundamental human right guaranteed under **Article 27(2) of the Constitution of the Republic of Uganda**. This constitutional protection is operationalised by the **Data Protection and Privacy Act, Cap 97** and the **Data Protection and Privacy Regulations, 2021**. The core rationale of data protection is to safeguard personal information, establish trust, ensure regulatory compliance, uphold ethical practices, and preserve individual autonomy. Central to this framework is the principle of consent, which must typically be obtained from the data subject before processing their personal data, barring specific lawful exceptions provided by the Act.

Children, however, occupy a uniquely vulnerable position. Due to their developing capacity, they are often unable to provide valid, informed consent. Consequently, special legal safeguards are essential. This article examines the legal framework for processing children's data in Uganda, explores the prevalent threats to their privacy, highlights regional enforcement developments, and identifies persistent challenges.

Legal Framework for Processing Children's Data in Uganda

The Data Protection and Privacy Act provides the specific regime for children's data in Section 8. It mandates prior parental or guardian consent for the collection and processing of a child's personal data. The section further stipulates that a child's data may be collected where it's necessary for compliance with the law or for research or statistical purposes.

A critical interpretation of Section 8 suggests that while parental consent is the primary gateway, the latter instances serve as alternative lawful bases for processing. However, it's a prevailing opinion that even these alternatives bases should, as a matter of best practice and heightened protection, still involve or consider parental awareness and engagement where possible, to fully align with the Act's protective spirit.

Uganda's framework is informed by and should be interpreted alongside key international instruments, including the UN Convention on Rights of the Child (UNCRC), which affirms the child's right to privacy, the African Charter on the Rights and Welfare of the Child (ACRWC), which provides a strong right to privacy and protection against unlawful interference, and the EU General Data Protection Regulation (GDPR), a leading model law whose principles of lawfulness, fairness, and data minimisation are instructive.

Threats and Violations: The Vulnerability of Children in the Digital Age

In an era of pervasive digital connectivity, children are increasingly exposed to social media, online gaming, and educational platforms, often facilitated by access to mobile devices. While these tools offer benefits, they also create significant risks as children may not fully comprehend privacy policies or the long-term implications of sharing personal information.

Types of children's data at risk may include (i) identifiers such as name, age, date of birth, photographs, videos, (ii) sensitive data such as location data, biometric data, education records, health information and (iii) digital footprints such as usernames, search histories, and social media interactions.

The misuse of this data leaves in open to exploitation, leading to severe potential consequences such as cyberbullying, psychological trauma, identity theft, online grooming, sexual exploitation, child trafficking, and impersonation. While adults can also fall victim to such violations, the impact on children is often more profound due to their developmental stage and vulnerability. Protecting children's data is therefore not merely a legal obligation but a critical component of safeguarding their overall dignity, safety, and well-being.

The different stakeholders have an important role to play in ensuring children's data protection. These include; i) the **Government** and the Regulator (PDPO) have a duty to enforce laws, issue clear guidelines on processing of children's data, and impose meaningful sanction. ii) **Parents and Guardians** ought to exercise reasonable supervision, educate children on digital literacy and privacy risks, and manage consent on their behalf. iii) **Schools and Institutions** should implement "privacy by design" to prevent exploitation of children's personal information, ensure lawful and secure data handling, and minimise data collection to only what is necessary and lastly iv) **Data Controllers and Processors** such as Tech Companies, Apps, etc should develop age-appropriate privacy notices, implement robust age-verification mechanism, and default to the highest privacy settings for children.

Recent Developments and Regional Enforcement Trends

- a. **Uganda:** The Personal Data Protection Office (PDPO) has yet to issue specific guidelines on processing children's data or a decision for violation of children's data. However, the Ministry of Education and Sports has proactively warned schools and media against publishing pupil or student results in ways that violate privacy which signals awareness on the issue.
- b. **Kenya:** The Office of the Data Protection Commissioner (ODPC) has published comprehensive "Guidance Notes on the Processing of Children's Data" which provide for children data protection considerations, safeguards for processing children data as well as obligations of data controllers and processors in processing children data. It has also enforced against data controllers for violations for example in **Julian Rowa (Suing on behalf of a minor) v The Nairobi Academy ODPC Complaint No. 1597 of 2025** where it found that the school had violation the child's privacy when it published the child's name and examination results in an advertisement feature of the Daily Nation newspaper without the consent of the parent and in absence of any lawful basis.

- c. **Tanzania:** The Personal Data Protection Commission (PDPC) has already demonstrated its willingness to protect children's privacy rights by issuing its first decision on children's privacy rights. In **Nyangoma Mwesingwa v Cecilia Maligaya Compliant No. PDPC/CMP/002/2025** it ruled that the use of a child's image for product advertising without parenta consent was a child privacy violation, clarifying that public availability of a child's photos on social media does not permit commercial use.

Challenges and Way Forward

Despite the existing framework, significant hurdles remain,

- a. **Weak enforcement and Limited Sanctions.** The capacity of the PDPO needs to be strengthened, potentially through granting it greater independence. Furthermore, the deterrent effect of penalties must be enhanced, and the regulator should be empowered to offer monetary compensation to victims .
- b. **Low Awareness and Digital Literacy:** There's widespread ignorance among children, parent and some institutions about privacy rights and risks. Existing awareness programs, such as BeeraKuGuard, must be intensified and expanded to reach grassroot communities to have a meaningful impact on the average Ugandan.
- c. **Regulatory Gaps:** The absence of specific guidelines on children's data creates uncertainty for data processors and leaves a significant gap. There is a need to borrow from Kenya's example by introducing detailed guidelines not only for children's data but also for various sectors to clarify lawful data processing.
- d. **Evolving Technology;** The rapid technology advancements continually outpace regulatory responses. This calls for the development of forward-looking laws that anticipate future trends and ensure the legal framework remains robust and adaptable.

Conclusion

Uganda has established a constitutional and statutory foundation for protecting children's data privacy, aligning with regional and global standards. However, the true test lies in effective implementation and enforcement. Learning from the proactive steps of our neighbouring regulators in Kenya and Tanzania, the PDPO must prioritise issuing clear guidelines and demonstrating a clear will to enforce the law. Ultimately, safeguarding children's privacy requires a concerted, ongoing effort from regulators, parents, educators, and the technology industry to translate legal principles into tangible protection for every child.

Author



Kemigisha Leticia

Research Associate

DPO Privacy Centre East Africa

kemigishaleticia1@gmail.com



Partner

