

Data Compliance Playbook for *Handling Children Data*



Data Compliance Playbook for Handling Children Data

1. Introduction

This Children's Data Compliance Playbook sets out the principles, obligations, and operational controls governing the processing of children's personal data by different stakeholders. The purpose of this playbook is to:

- tell you what the law says about children's data rights and protection
- give you practical guidance on how to deal with children's data
- ensure safety in all children's data processing activities
- embed privacy by design into products and services involving children
- reduce regulatory, legal, and reputational risk

An organisation can adopt it as an operational guide and a compliance resource to aid audits, investigations or regulatory engagements.

Children's data rights and protection is governed under these Nigerian laws:

- Constitution of the Federal Republic of Nigeria, 1999 as amended
- Child Rights Act, 2003 or respective State laws.
- Nigeria Data Protection Act (NDPA), 2023
- NDPA General Application and Implementation Directive

2. Who the Playbook Serves

2.1. Are you a:

- a. Parent
- b. Educational Institution,
- c. Platform owner,
- d. Financial institution,
- e. Travel agency, or
- f. Religious institution?

Or do you interact with children's personal data, directly or indirectly? Then, this is for you.

2.2. Applicability Criteria

In a simpler form, do you:

- a. Offer services directly to children, or
- b. Offer mixed-audience services reasonably likely to be accessed by children, or
- c. Process children's data indirectly (e.g., through parents, schools, guardians),
- d. Process children's data on behalf of another controller (processor role); or
- e. Have a responsibility of giving consent on behalf of children?

Then, this is for you.

3. Who is a Child? What are their data rights and how can you protect them?

- 3.1. This section ensures all stakeholders apply the correct legal threshold and understand that children receive heightened protection under the NDPA.
- 3.2. Under Nigerian law, a child is any individual under the age of 18 years.
- 3.3. The Rights of a child in the digital age includes:
 - i. Right to Privacy¹: Every child is entitled to his privacy, family life, home, correspondence, telephone conversation and telegraphic communication.²
 - ii. Right to freedom from discrimination: child shall not be subjected to any form of discrimination merely by reason of his belonging to a particular community or ethnic group or by reason of his place of origin, sex, religion or political opinion.³
 - iii. Right to dignity of the child: Every child is entitled to respect for the dignity of his person, and accordingly, no child shall be subjected to attacks upon his honor or reputation.
 - iv. Right to freedom of expression.

4. Processing a Child's Data: Day-to-day Examples

S/N	Stakeholder	Examples
1.	Parents/Legal guardians	- Providing consent on behalf of children where required under law (e.g. before accessing

¹ Section 37 CRFN, 1999 (as amended)

² Section 8(1) CRA, 2003

³ Section 10 CRA, 2003

S/N	Stakeholder	Examples
		<p>YouTube Kids, or Netflix Kids)</p> <ul style="list-style-type: none"> - Managing and safeguarding children’s login credentials or access device. - Granting or withdrawing access to children’s data by platform owners or third parties. - Exercising data subject rights on behalf of children (access, correction, deletion). - Communicating children’s special needs or preferences.
2.	Educational Institutions	<ul style="list-style-type: none"> - Collection of enrolment and admission data. - Academic records and attendance tracking. - Health data processing to support children with special medical needs. - Biometric data collection (e.g. fingerprints, facial images) for identification, access control, or attendance. - Communication with parents or guardians regarding student welfare.
3.	Financial Institutions	<ul style="list-style-type: none"> - Processing identification information linked to children (e.g. National Identification Number (NIN)). - Management of child-linked bank accounts or savings products. - Processing limited financial transaction data. - Compliance with KYC and regulatory obligations involving minors.
4.	Government Agencies	<ul style="list-style-type: none"> - Identity verification and civil registration (birth registration, NIN enrolment). - Education, health, or social welfare program enrolment. - Collection of demographic data for public services. - Lawful monitoring or record-keeping mandated by statute.
5.	Religious Institutions	<ul style="list-style-type: none"> - Registration of children for religious programs, classes, or events. - Collection of basic identification and contact information. - Processing health-related information for children with special needs during programs or camps. - Emergency contact and welfare management.
6.	Platform owners	<ul style="list-style-type: none"> - Account creation and user authentication for child or child-linked accounts. - Delivery of digital services (educational, entertainment, social, or informational). - Collection of usage and interaction data. - Implementation of safety, moderation, and

S/N	Stakeholder	Examples
		content controls. - Analytics and service improvement. - Communication with parents or guardians. - Compliance monitoring and fraud prevention.

5. Processing a Child’s Data: Best Practices and Principles

Stakeholder	Key Data Processing Activity	Applicable Data Protection Requirement / Principle
Parents / Legal Guardians	Providing consent on behalf of children ⁴	Consent must be informed, specific, and verifiable; processing must align with the best interests of the child. ⁵
	Managing children’s login credentials or access	Security and confidentiality obligations; prevent unauthorised access to the child’s data ⁶
	Exercising data subject rights for children	Right of access, rectification, and erasure must be facilitated without undue delay.
Educational Institutions	Collection of enrolment and academic records	Lawfulness and purpose limitation; data collected strictly for educational purposes
	Processing health data of students	Sensitive personal data protection; enhanced security and access restrictions required.
	Use of biometric data for attendance or access	Necessity and proportionality; biometric data only where no less intrusive alternative exists.
Financial Institutions	Processing children’s identification data (e.g. NIN)	Lawful basis and data minimisation; collect only what is required for regulatory compliance.
	Management of child-linked accounts and transactions	Accuracy and security; ensure data is current and protected against fraud
Religious Institutions	Registration of children for programmes	Purpose limitation and data minimisation; collect only basic necessary data.
	Processing health data for children with special needs	Confidentiality and integrity; restricted access and secure handling.
Government Agencies	Identity verification and civil registration	Legal obligation and public interest; processing must be authorised by law.

⁴ Section 31 NDPA, 2023

⁵ Article 17 NDPA GAID, 2025

⁶ Section 39, NDPA

Stakeholder	Key Data Processing Activity	Applicable Data Protection Requirement / Principle
	Enrolment in social or public welfare programmes	Transparency and accountability; clear communication of purpose and retention.
Platform Owners / Service Providers	Account creation and authentication for children	Privacy by design and by default; high-privacy settings enabled by default.
	Collection of usage and interaction data	Data minimisation and fairness; avoid excessive tracking or profiling.
	Use of analytics, AI, or recommendation systems	Restriction on profiling of children; avoid automated decision-making that may harm children.
	Communication with children or parents	Transparency and age-appropriate communication; clear, simple language.
	Data retention and deletion	Storage limitation; children's data retained only as long as necessary.

6. Compliance Checklist

The following checklist outlines the minimum compliance actions required when processing children's personal data, in line with the Nigeria Data Protection Act 2023 (NDPA) and applicable child protection principles.

Compliance Obligation	Compliance Status
Appointment of a Data Protection Officer (DPO) ⁷	
Appointment of a Data Protection Compliance Organisation to conduct annual compliance audit ⁸	
Conduct a Data Protection Impact Assessment (DPIA) ⁹	
Determine Lawful Basis for Processing ¹⁰	
Parental or Guardian Consent (Where Applicable) ¹¹	
Age Verification Mechanisms ¹²	
Transparent and Accessible Privacy Notices	
Data Minimisation ¹³	
Privacy by Design and by Default	
Technical and Organisational Measures ¹⁴	
Grievance Redress Mechanism	

⁷ Section 32 NDPA, 2023

⁸ Section 33, NDPA 2023, Article 7 NDPA GAID, 2025

⁹ Section 28, NDPA, 2023

¹⁰ Section 25, NDPA, 2023

¹¹ Section 31, NDPA, 2023

¹² Section 31, NDPA 2023

¹³ Article 15, NDPA GAID, 2025

¹⁴ Section 39, NDPA 2023,

7. Conclusion

The protection of children’s personal data is a legal, ethical, and organisational responsibility. Under the Nigeria Data Protection Act 2023, the Child Rights Act, and the oversight of the Nigeria Data Protection Commission, organisations that process children’s data are required to apply heightened safeguards and to prioritise the best interests of the child at all times.

¹⁵ Article 30, NDPA, 2023



About *Firm*

HAMU Legal is a business-oriented law firm, with innovation, technology and a better way of providing legal services at its heart.

We are legal partners to individuals, early-stage companies, and established companies looking for counsel they can trust. We take pride in providing pragmatic and agile legal counsel to clients who are game-changers that believe in disrupting the status quo, in the pursuit of creating impact in their various sectors.

We are driven by our passion for the law and an entrepreneurial spirit to adapt to the changing demands with regards to how legal services are delivered. At HAMU Legal, our clients are more than just clients – they are our partners. Regardless of how long you have been in partnership with us, we are always here to provide excellent, bespoke services to cater for your legal needs.

This article is only intended to provide general information on the subject matter and does not by itself create a client/attorney relationship between readers and Hamu Legal or serve as legal or financial advice.

We are available to provide specialist legal advice on the readers' specific circumstances when they arise. For further enquiries, please reach out to our Intellectual Property and Technology team at awuese@hamulegal.com or team@hamulegal.com.



6 Cairo Crescent, House 9B
Off Adetokunbo Ademola Cr,
Wuse 2, Abuja.



people@hamulegal.com



+234 906 000 5026