

Strategic legal Considerations under the Internet Code of Practice 2026

Regulatory Update

The Internet Code of Practice 2026 ("**2026 Code**"), which came into effect on February 13, 2026, marks a significant milestone in Nigeria's digital regulatory landscape. Issued by the Nigerian Communications Commission (NCC) pursuant to Section 70 of the Nigerian Communications Act 2003 (the Act), the 2026 code replaces the Internet Code of Practice 2019 ("**2019 Code**"). The 2026 Code reflects a more complex and interconnected digital ecosystem, recognising that internet governance now extends beyond traditional Internet Access Service Providers (IASPs) to a wider range of digital actors.

Alongside the 2026 Code, the Commission published Guidance Notes for the Implementation and Enforcement of the Internet Code of Practice 2026 (Guidance Notes) to clarify regulatory expectations, implementation timelines, and operational processes. The Guidance Notes are subordinate to the Code and are to be read alongside it.

From a policy perspective, the 2026 Code illustrates the NCC's intent to adopt a more proactive regulatory approach. However, while the framework is ambitious, its effectiveness will depend on how clearly obligations are interpreted, the capacity of regulated entities to comply, and the consistency of enforcement.

Therefore, this article highlights the key provisions of the 2026 Code and the Guidance Notes, drawing attention to the changes introduced relative to the 2019 Code, as well as practical actions that telecommunications companies ought to consider.

2026

Code in force
13 February 2026

180d

To full enforcement
Phased rollout

12+

New obligations
for IASPs & platforms

Contributors



**Okechukwu
Ekweanya**

Partner, Corporate
Governance & Regulatory
Compliance



Chidera Mbaogu

Associate, Corporate
Governance & Regulatory
Compliance



**Chinemenma
Igbokwe**

Associate, Corporate
Governance & Regulatory
Compliance

For further information on the issues discussed in this article,
contact our legal team at counsel@kennalp.com

Scope of Application and Enforceability

A major departure from the 2019 Code is the expansion of regulatory scope. While the earlier regime applied exclusively to Internet Access Service Providers ("IASPs"), the 2026 Code extends its obligations to "impacted entities," including digital platforms, application providers, and other actors operating over telecommunications networks that are affected by the regulatory provisions of the Nigerian Communications Act 2003.²

This expansion has important implications. First, it effectively brings previously unregulated or lightly regulated digital service providers within the NCC's oversight. This reflects global regulatory trends where platform governance is no longer treated as separate from telecommunications governance.

However, the distinction between licensees (subject to strict enforcement) and impacted entities (subject to a "soft" governance approach)³. The absence of clear thresholds for determining when collaborative compliance may transition into enforcement could create uncertainty. Entities may struggle to assess their risk exposure, particularly where their classification evolves with business growth or service expansion.

In practice, companies will need to adopt a cautious approach by treating "soft" obligations as effectively binding, especially given the reputational and regulatory risks associated with non-compliance.

Two enforcement tiers

Licensees

Strict enforcement

IASPs and other holders of NCC licences are subject to the Code's **full enforcement regime**, including sanctions for non-compliance.

Impacted Entities

Soft governance

Digital platforms, application and service providers — engaged through a **collaborative compliance** approach.

Key Addition

Objectives of the Code:

The Code now additionally seeks to ensure that Online Platforms and Digital Services align their activities with the national regulatory environment through cohabiting governance rules that provide clear guiding principles for their operations.⁴

This development is significant because it signals the NCC's intention to influence not only infrastructure providers but also content ecosystems and digital behaviour. However, it may lead to jurisdiction overlaps with other regulators, particularly in areas such as data protection.

Data Breach Notifications:

The 2026 Code refines the breach notification framework in two key respects. First, the trigger for customer notification is shifted from "within 48 hours of occurrence" (as in the 2019 Code) to "within 48 hours of becoming aware of the breach," a practically significant change.⁷ Second, a two-stage notification mechanism is introduced where full details are unavailable, the IASP must issue a preliminary notification within the 48-hour window and furnish a comprehensive update within 14 days, or within any extended period approved by the Commission.

However, the coexistence of the 48-hour threshold under the Code and the 72-hour threshold under the Nigerian Data Protection Act (NDP Act) creates potential compliance complexity. Organisations may face dual reporting obligations requiring careful coordination to avoid inconsistencies. In practice, companies may need integrated incident response systems that simultaneously satisfy telecoms and data protection requirements. Internet Code of Practice, 2026; Section 3.4, 'Data Breach Notifications'

No Preferential Data Prioritisation:

The 2019 Code imposed an absolute prohibition on preferential data prioritisation.⁵ The 2026 Code introduces a conditional approach: an IASP may not engage in such prioritisation without the Commission's prior written regulatory approval.⁶

Nonetheless, discretionary approval introduces regulatory uncertainty, as without clearly defined criteria, operators may face delays or inconsistent outcomes in obtaining approval.

48hrs

Preliminary notice
from awareness

14days

Comprehensive
follow-up update

72hrs

NDP Act threshold
requires dual reporting

Transactional Data Management:

This is an entirely new provision. IASPs are now prohibited from allowing the harvesting of transactional data on their networks or from granting third parties access to it without prior written approval from the Commission, preceded by an impact assessment. Transactional data is broadly defined to include metadata, user activity logs, usage patterns, communication details, and behavioural data that may be used for billing, analytics, or regulatory compliance.⁸

Incorporation of Child Online Protection Policies into Terms and Conditions of Service:

The 2026 Code significantly extends responsibilities to all impacted, requiring the provision of accessible parental control tools, multilingual safety guidance, and the adoption of default opt-in settings before services are provided to minors and vulnerable dependents.⁹

Transactional data — broadly defined

Metadata

User activity logs

Usage patterns

Communication details

Behavioural data

Used for billing, analytics, or regulatory compliance.

Takedown Notice:

The 2019 Code provided only blanket takedown notices to all IASPs upon the Commission's determination that content was unlawful. The 2026 Code retains this mechanism but also introduces a targeted approach, enabling the Commission to issue a notice to a specific IASP regarding content that pertains only to that provider. Both mechanisms require compliance within 24 hours of receipt.¹⁰

24hrs

Compliance window

Both **blanket and targeted** takedown mechanisms require compliance within **24 hours** of receipt.

Deployment of AI & Emerging Technologies:

A wholly new provision in the 2026 Code, being a timely inclusion, is the regulation of Artificial Intelligence (AI) and emerging technologies. IASPs are now required to obtain regulatory notification before deployment and provide details on their scope, impact on existing services, and implementation timelines. By requiring prior notification and emphasising transparency and data protection, the NCC positions itself at the forefront of AI governance.¹²

However, the Commission's power to direct the withdrawal of AI systems is notably broad and potentially disruptive, particularly where such systems are already embedded in core service delivery. The absence of clearly defined procedural safeguards, including a right to be heard or a procedure for intervention, creates a real risk of regulatory overreach and uncertainty for operators.

Additionally, the Commission is expected to review such notifications and provide feedback within 15 days.¹³

Objectives of the Code:

The 2026 Code introduces the appointment of a DOGO within the NCC to serve as the central point of contact for managing harmful content and other unlawful online activities. Licensees and impacted entities are required to designate a regulatory focal person to maintain a direct point of contact with the DOGO. This requirement forms part of the organisational compliance obligations that must be implemented within the 90-day gestation period following the Code's publication in February 2026.¹⁵

Online and Digital Platforms Governance:

The 2026 Code introduces a new framework on Online and Digital Platforms Governance, extending regulatory obligations beyond IASPs to include online platforms, digital service providers, and application service providers. Thus, every online and digital platform must adopt community rules or guidelines aligned with Section 146 of the NCC Act and submit them to the Commission within six months of the Code's issuance.¹⁶

They must also provide biannual compliance reports (renditions) and establish a direct engagement channel with the DOGO to address issues such as harmful content, disinformation, and unlawful activities.¹⁷

Community guidelines

Aligned with Section 146 NCC Act — submitted within 6 months.

Biannual compliance reports

Renditions filed every six months to the Commission.

DOGO engagement channel

Direct line for harmful content, disinformation, unlawful activities.

Rendition Requirements:

The 2026 Code introduces formal rendition (reporting) obligations to strengthen compliance monitoring. IASPs are required to submit biannual compliance reports, while both IASPs and impacted entities must also provide specific compliance reports in response to regulatory requests. The Guidance Notes provide that rendition submissions will be reviewed and feedback given within 15 days.²⁰

Biannual reports

Every six months — covering operations, incidents and compliance.

Ad-hoc compliance reports

Filed on demand, in response to regulatory requests.

Electronic Addressing Management:

IASPs are now required under the 2026 Code to document and submit all Internet Protocol (IP) addresses deployed on their networks to the Commission every month, maintain utilisation records of all IP addresses and submit these monthly, and report to the Commission any IP address deployed in breach of the Code or Section 128 of the NCC Act.²¹

This provision strengthens the Commission’s ability to monitor network usage and detect potentially unlawful deployments.

Compliance Timelines:

The Guidance Notes prescribe a phased implementation timeline. Phase 1 is a 90-day regulatory gestation period from February 13, 2026, during which stakeholders prepare for compliance, appoint regulatory focal persons, and set up DOGO engagement channels, with no enforcement action during this period. Phase 2 is a further 90-day compliance period during which entities must submit their first renditions and align operations with the Code. Phase 3 commences 180 days from publication, marking the start of full compliance monitoring and enforcement, with possible sanctions for non-compliance.²² By August 12, 2026, Phases 2 and 3 must be implemented by the concerned organisations.

Phase 1

Regulatory Gestation

90 days from 13 February 2026

Phase 2

Compliance Period

Further 90 days after Phase 1

Phase 3

Full Enforcement

180 days from publication

Practical Compliance Steps for Telecommunications Companies and Impacted Entities

In response to the 2026 Code, organisations should prioritise the following practical compliance actions:

01 Policy gap review

Review existing policies against the 2026 Code to identify and address gaps in data protection, content governance, AI use, and reporting obligations.

02 Designate a regulatory focal person

Designate a regulatory focal person within the company to liaise with the DOGO and to ensure effective implementation of the 2026 Code.

03 Update breach notification procedures

Update breach notification procedures to reflect the 48-hour awareness threshold and two-stage reporting requirement, while still ensuring compliance with the NDP Act.

04 Develop community guidelines

Develop and implement community guidelines and submit these guidelines to the Commission within six months of the issuance of the Code.

05 Stand up biannual reporting

Establish systems for biannual reporting and ensure timely submission of compliance reports.

06 Review AI & emerging-tech deployments

Review AI and emerging technology deployment practices, ensuring prior notification to the Commission.

07 Train your stakeholders

Engage in training for stakeholders and employees on new obligations under the 2026 Code.

Conclusion

The 2026 Internet Code of Practice represents a fundamental expansion of Nigeria's digital regulatory framework, shifting from a narrow, IASP-focused regime to a comprehensive framework governing the broader digital ecosystem. Its new provisions on artificial intelligence, transactional data, platform governance, and online child safety, together with the structured reporting and enforcement mechanisms introduced, signal a more proactive and forward-looking approach to digital oversight. The Guidance Notes provide the practical implementation architecture, and stakeholders, particularly those newly classified as impacted entities, should carefully review their obligations and act within the prescribed timelines.

For further information

Speak with the KENNA legal team about preparing for the 2026 Code.

Endnotes

1. Internet Code of Practice, 2026; Section 1.1, 'Preamble'
2. Internet Code of Practice, 2026; Section 1.4, 'Application and Scope of the Code, Section 8, 'Interpretation of Key Terms'. Under the code an "impacted entity" is defined as any person or entity that does not hold an individual licence from the Commission but provides any service within the purview of the Nigeria Communications Act.
3. Guidance Notes for the Implementation and Enforcement of the Internet Code of Practice 2026; Section 2 (6), 'Compliance Monitoring and Enforcement'
4. Internet Code of Practice, 2026; Section 1.3, 'Objectives of the Code'
5. Internet Code of Practice, 2019; Section 3.5, 'No Preferential Data Prioritisation.'
6. Internet Code of Practice, 2026; Section 2.5, 'No Preferential Data Prioritization'
7. Internet Code of Practice, 2026; Section 3.4, 'Data Breach Notifications'
8. Internet Code of Practice, 2026; Section 3.5, 'Transactional Data Management'
9. Internet Code of Practice, 2026; Section 4.1, 'Incorporation of Child Online Protection Policies into Terms and Conditions of Service'
10. Internet Code of Practice, 2026; Section 5.3.3, 'Takedown Notice'
11. Internet Code of Practice, 2026; Section 5.4.1, 'Deployment of Artificial Intelligence on the Network'
12. Internet Code of Practice, 2026; Section 5.4.2, 'Regulatory Requirements for the Deployment of Artificial Intelligence'
13. Guidance Notes for the Implementation and Enforcement of the Internet Code of Practice 2026; Section 3 (2), 'Rendition on Artificial Intelligence'
14. Guidance Notes for the Implementation and Enforcement of the Internet Code of Practice 2026; Section 4 (1), 'Appointment of a Designated Online Governance Officer'
15. Ibid
16. Internet Code of Practice, 2026; Chapter 6, 'Online and Digital Platforms Governance Rules'
17. Ibid
18. See the First Schedule of the Internet Code of Practice, 2026
19. See the Third Schedule of the Internet Code of Practice, 2026
20. Guidance Notes for the Implementation and Enforcement of the Internet Code of Practice 2026, Paragraph 5.3
21. Internet Code of Practice, 2026; Section 2.8, 'Electronic Addressing Management'
22. Guidance Notes for the Implementation and Enforcement of the Internet Code of Practice 2026



CONTACT US

LAGOS

KENNA Place
8, Ogunyemi Road, Palace Way,
Oniru PO Box 73002,
Victoria Island, Lagos

ABUJA

1st Floor, Novare Central
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285,
Abuja

ENUGU

Michael Place
3, Emmanuel Ngwu Street,
Thinker Corner,
400211 Enugu State.

+234 811 395 1052, +234 811 395 1053 | counsel@kennalp.com