KENNA

Data Protection Practice Unit

Newsletter – Volume 1

A review of the 2026 judicial, regulatory and thought-leadership developments shaping Nigeria's data protection landscape



Editor's Note

Welcome to the 2026 Edition, Volume 1 of the KENNA Data Protection Practice Unit Newsletter.

The first half of 2026 has been a defining period for data protection law and enforcement, both in Nigeria and across the international regulatory landscape. This edition captures the key judicial pronouncements, regulatory developments, and thought leadership shaping the discourse in this critical area of practice.

In our "From the Court" section, we examine five landmark decisions that collectively reinforce the fundamental principles underpinning data protection law. From the Nigerian courts, we analyse the Federal High Court's decision in Onimisi v Guaranty Trust Holding Company, which affirmed the sanctity of consent and the right to erasure in the context of unsolicited communications, and the Lagos High Court's ruling in Agboola v Fidelity Bank Plc, which drew a firm line against the repurposing of personal data beyond the scope of original consent under the Global Standing Instruction framework. We also consider the significant judgment in Femi Falana, SAN v Meta Platforms, where the court imposed vicarious liability on a social media platform for third-party content that infringed upon an individual's privacy rights, a decision with far-reaching implications for digital intermediaries.

Beyond Nigeria, we review the UK Court of Appeal's decision in DSG Retail Ltd v Information Commissioner[1], which clarified that the data controller must assess whether data is "personal", regardless of whether a third-party attacker can identify the data subjects. We also examine the Irish High Court's judgment in TikTok Technology Limited v Data Protection Commission, which reaffirmed the General Data Protection Regulation's (GDPR) stringent requirements for cross-border data transfers and underscored the extraterritorial reach of data protection obligations.

Our regulatory updates section reflects the Nigeria Data Protection Commission's (NDPC) growing dynamism. We report on the NDPC's investigation into Temu's data processing practices, its advisory on escalating cybersecurity threats, the launch of the Meta-Supported Initiative for Data Protection (M-SIDP), and the Commission's guidance on continuous professional development for Data Protection Officers. We also highlight the Central Bank of Nigeria's new data localisation requirements for fintech operators. From the European Union, we cover developments including the EDPB's joint opinion on the Digital Omnibus Regulation, the standardised DPIA template consultation, guidelines on scientific research processing, the approval of the Europrivacy certification scheme for international transfers, age verification initiatives, and the phased implementation of AI Act obligations.

Finally, in our publications section, we spotlight our team's thought leadership on key compliance challenges: the 2026 data protection outlook, annual audit return obligations, data processing agreements under the Nigeria Data Protection Act (NDP Act), and legal strategies for data breach response and resilience.

We trust that you will find this edition insightful and valuable.

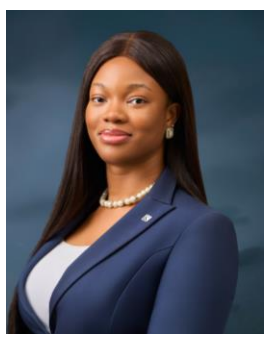
> *"The first half of 2026 has been a defining period for data protection law and enforcement, both in Nigeria and across the international regulatory landscape."*



Nimma Jo-Madugu, CIPP/E
Partner, Data Protection Practice Unit



Chidera Ezenwanne, ACArb
Senior Associate,
Data Protection Practice Unit



Chineme Igbokwe
Associate, Data Protection Practice Unit

From the Courts - *Nigeria*

Consent, lawfulness and right to erasure

- Abdulmalik Muhaimin Onimisi v Guaranty Trust Holding Company[2]

In a landmark judgment delivered by the Federal High Court, Abuja Judicial Division on June 11, 2026, the Court held that Guaranty Trust Holding Company (GTCO) was liable for sending unsolicited messages to the Applicant, who was not a customer of the bank.

On April 9, 2025, the Applicant received an unsolicited promotional SMS from a GTCO subsidiary, Guaranty Trust Fund Managers, offering returns on savings through its "Fund 724" product, despite never being a customer of the Respondent or having provided his personal data to it. The message also lacked an opt-out mechanism. The Applicant requested disclosure of the data source, cessation of all marketing communications and deletion of his personal data from their databases. Despite complaining to the Respondent and requesting erasure of his data from its platform, he received another promotional SMS on April 23, 2025, while the complaint remained pending. Consequently, the Applicant commenced this action alleging unlawful processing of his personal data and violation of his right to privacy.

In its judgement, the court held that GTCO violated the Applicant's privacy rights by sending unsolicited messages without the Applicant's consent. The court further held that the Applicant, as a data subject, has the right to request the deletion of his data from GTCO's database. On the issue of obtaining the Applicant's data without permission, the court ordered GTCO to disclose the source from which the Applicant's personal data was obtained, including any third parties involved.

This case upholds the principle that a data processor or controller must establish a lawful basis for processing personal data and, where consent is the only available basis, personal data cannot be processed without it. The court affirmed that organisations must respect individuals' data protection rights and ensure compliance with the NDP Act. The judgment further strengthens the right to erasure by confirming that data subjects may require organisations to delete their personal data where its continued processing is unlawful or unjustified.

AT A GLANCE

Court
Federal High Court, Abuja Judicial Division

Judgment date
June 11, 2026

Issue
Unsolicited marketing messages; consent; source of personal data

Framework
Nigeria Data Protection (NDP) Act

> *Where consent is the only available basis, personal data cannot be processed without it.*
>
> **Federal High Court, Abuja**

Purpose limitation and lawful processing

- Esther Agboola v Fidelity Bank Plc[3] Suit No: LD/19478MFHR/2025

In the judgement delivered on February 12, 2026, the High Court of Lagos State considered whether Fidelity Bank Plc (Bank) violated the Applicant's constitutional right to privacy and the provisions of the NDP Act by processing her personal and financial data under the Global Standing Instruction (GSI) framework.

The dispute arose from the Respondent's processing of the Applicant's bank account to automatically recover a loan pursuant to the Global Standing Instruction (GSI) framework. The Applicant contended that she neither obtained the loan allegedly giving rise to the debt nor executed any GSI mandate authorising the recovery. She further maintained that she did not consent to or authorise the debit of ₦11,922.41 (Eleven thousand, nine hundred and twenty-two naira, forty-one kobo) from her bank account.

In its judgment, the Court held that the Bank failed to discharge the burden of proof that the Applicant had obtained the alleged loan or executed any GSI mandate. The Court further held that the Bank's disclosure, processing, and use of the Applicant's financial information for loan recovery without establishing a lawful basis violated her right to privacy under Section 37 of the Constitution of the Federal Republic of Nigeria (1999) as amended and violated the principles of fairness, accuracy, and lawfulness under Sections 24 and 25 of the NDP Act.

The judgment upholds the principle that consent obtained for one purpose cannot be treated as blanket or omnibus consent for unrelated processing activities. In other words, organisations cannot rely on a data subject's prior consent to justify a subsequent use or processing of such personal data for a purpose that falls outside the scope of the original purpose for which the consent was granted. In the present case, although the Bank lawfully possessed and processed the Applicant's personal data to operate and maintain her bank account, that consent did not automatically extend to processing her data for automatic loan recovery under the Global Standing Instruction (GSI) framework.

AT A GLANCE

Court
High Court of Lagos State

Judgment date
February 12, 2026

Issue
Automatic loan recovery under the Global Standing Instruction (GSI) framework

Amount in dispute
₦11,922.41 debited without authorisation

Practical takeaway

Consent obtained for one purpose cannot be treated as blanket or omnibus consent for unrelated processing activities — prior consent does not automatically extend to a purpose outside the scope of the original grant.

Constitutional anchor

Section 37, Constitution of the Federal Republic of Nigeria (1999) as amended — right to privacy

Statutory anchor

Sections 24 & 25, NDP Act — principles of fairness, accuracy and lawfulness

Framework

Global Standing Instruction (GSI) — automatic loan recovery across accounts

Lawfulness, fairness and accountability

- Femi Falana, SAN v Meta Platforms[4]

In a landmark judgement delivered on January 13, 2026, the Lagos State High Court held Meta liable for privacy and data breaches arising from third-party content published on Facebook.

The Applicant's complaint was centred around the video captioned **"AfriCare Health Centre",** which made unauthorised use of the Applicant's name, photograph, and motion images. In the video, the Applicant was portrayed as introducing himself by name and claiming that he had been treating prostatitis for over sixteen years. The Applicant contended that the video's representations were false and that he neither participated in nor consented to the creation, publication, or dissemination of the content.

The Court held that the Respondent is vicariously liable for the publication placed on its platform by third parties. The Court further held that the Respondent, which hosts third-party information on its platform for valuable consideration, owes a correlative obligation to ensure that publications posted on its platform by undisclosed third parties do not conflict with others' right to privacy as guaranteed in the Constitution.

This case underscores the increased responsibility of social media platforms and other digital intermediaries to ensure that personal data published on their platforms is processed in compliance with data protection laws. Importantly, the judgment demonstrates that the defence that content was uploaded by an independent third party may not, without more, absolve a platform of liability where it continues to host, process, disseminate, or retain such content after becoming aware of the infringement.

AT A GLANCE

Court

Lagos State High Court

Judgment date

January 13, 2026

Issue

Vicarious liability for third-party content infringing privacy rights

Platform

Facebook — video captioned "AfriCare Health Centre"

Why it matters

Hosting, processing, disseminating or retaining infringing third-party content after becoming aware of it may expose a platform to liability — the "independent third party" defence may not, without more, absolve it.

From the Courts – *United Kingdom*

Data security and integrity/confidentiality

- DSG Retail Ltd v Information Commissioner [5]

In this judgment, the Court of Appeal, delivered on February 19, 2026, considered the scope of a data controller's duty to protect data subjects' personal data, particularly in the context of cyberattacks and data security breaches.

The appeal arose from a cyberattack on DSG Retail Limited's ("DSG") systems, the owner and operator of well-known retail brands including Dixons and Currys PC World, between 2017 and 2018. During the attack, cybercriminals infiltrated DSG's systems and, over about nine months, obtained millions of customers' payment card data. However, the vast majority of the compromised cards were protected by chip-and-pin technology; as such, the attackers obtained only the PAN and expiry date and did not obtain the cardholder's name or other information capable of directly identifying the cardholder.

The Court of Appeal was then asked whether the compromised data constituted personal data, even though the attackers could not, on the information obtained, identify the individuals to whom the data related. DSG argued that, because the attackers could not identify the specific individuals from the data alone, the information did not constitute personal data in the attackers' hands.

The Court held that, in determining whether a data breach occurred, the relevant question is whether the compromised data constitutes personal data under the data controller's control, not a third party's, regardless of whether a third-party attacker can identify the individuals concerned. Because the data accessed by the hackers constituted personal data under DSG's control as the data controller, DSG breached its security obligations to protect the personal data of subjects.

This judgment reaffirms the stringent obligations imposed on data controllers and data processors to implement appropriate technical and organisational measures to safeguard personal data against unauthorised access, disclosure, loss, or compromise.

Importantly, the Court clarified the scope within which a data breach is to be assessed for data protection law. The fact that compromised data may not identify the data subject in a hacker's hands does not necessarily deprive it of its character as personal data. Where information constitutes personal data from the perspective of the data controller or processor that holds it, data protection law's protections remain applicable.

AT A GLANCE

Court
Court of Appeal (England & Wales)

Judgment date
February 19, 2026

Issue
Whether compromised payment card data constituted personal data

Attack window
2017–2018, around nine months of infiltration

Obtained by attackers

PAN and expiry date — cards largely protected by chip-and-pin technology

Not Obtained

Cardholder's name or other information capable of directly identifying the cardholder

Cross-border transfers and transparency

- TikTok Technology Limited & Anor v Data Protection Commission [6]

This appeal judgment delivered on June 3, 2026, provided clarity on the application of the General Data Protection Regulation's (GDPR) cross-border data transfer requirements and the extent of a data controller's obligations to ensure that personal data transferred outside the European Economic Area (EEA) is afforded a level of protection essentially equivalent to that guaranteed under EU law.

The appeal arose from an inquiry conducted by the Irish Data Protection Commission (IDPC) into TikTok's cross-border data transfer arrangements and processing practices. The inquiry was initiated following concerns that TikTok's transfer of personal data belonging to users within the EEA to China might not comply with the GDPR's framework governing international transfers of personal data. In particular, the IDPC examined whether personal data accessed from China through remote access arrangements was adequately protected against potential interference and unauthorised access in accordance with the GDPR's standards.

In its judgment, the Court upheld the Irish Data Protection Commission's (IDPC) decision and found that TikTok infringed Articles 46(1) and 13(1)(f) of the General Data Protection Regulation (GDPR). The Court held that TikTok failed to demonstrate that the personal data of users transferred through remote access to China was afforded a level of protection essentially equivalent to that guaranteed under the GDPR. The Court further held that TikTok breached its transparency obligations under Article 13(1)(f) of the GDPR by failing to adequately inform users that their personal data could be transferred to, or remotely accessed from, China.

This case highlights the importance of strict compliance with a jurisdiction's data protection laws, particularly regarding cross-border transfers of personal data. Organisations transferring personal data outside any jurisdiction must ensure that the transferred data continues to enjoy a level of protection essentially equivalent to that guaranteed under the applicable data protection law in the jurisdiction from which the data was transferred.

The decision also underscores that data protection obligations follow personal data originating from a particular jurisdiction. In this instance, the GDPR transfer rules continued to apply to personal data processed in China because the data had been collected from individuals within the EEA and transferred from that region. The case therefore demonstrates that organisations cannot evade their data protection obligations merely by transferring data to countries outside the territorial scope of the applicable data protection law.

AT A GLANCE

Court
High Court of Ireland

Judgment date
June 3, 2026

Issue
EEA-to-China transfers; remote access; adequacy of protection

Attack window
Articles 46(1) & 13(1)(f), GDPR

> *"Data protection obligations follow personal data originating from a particular jurisdiction.*
>
> **High Court of Ireland**

Contributors



Oluwapelumi Ikujenyo
Associate



Michael Arinze
Associate

Regulatory Updates - *Nigeria*

NDPC Commences Investigation into Temu's Data Processing Practices

On February 17, 2026, the Nigeria Data Protection Commission (NDPC) announced it had begun an investigation into Temu, the Chinese-owned e-commerce platform, over suspected violations of the NDP Act, 2023.

According to the Commission, concerns were raised about Temu's data processing activities, including alleged online surveillance practices, opaque data-handling procedures, cross-border transfers of personal data, and potential breaches of the data minimisation principle. The investigation is particularly significant given the platform's substantial footprint in Nigeria, where it reportedly processes the personal data of approximately 12.7 million Nigerians.[7]

The development shows the NDPC's growing willingness to subject multinational technology companies operating in Nigeria to regulatory scrutiny. It also signals that transparency, international data transfers, and accountability remain key enforcement priorities under the NDP Act.

For organisations operating digital platforms or conducting large-scale data processing in Nigeria, the investigation reminds them to maintain robust governance structures, transparent privacy practices, and lawful cross-border transfer mechanisms.

Reported footprint in Nigeria

12.7m

Nigerians whose personal data Temu reportedly processes — underscoring the scale of the investigation.

Focus of the probe

- *Alleged online surveillance practices*
- *Opaque data-handling procedures*
- *Cross-border transfers of personal data*
- *Potential breaches of the data minimisation principle*

NDPC Issues Advisory on Escalating Cybersecurity Threats

On April 16, 2026, the NDPC issued a Data Protection Advisory[8] in response to increasing threats targeting Nigeria's digital infrastructure and financial systems. The Commission said threat actors had engaged in coordinated cyber operations targeting critical digital assets and reminded organisations of their obligations under the NDP Act to implement appropriate technical and organisational measures to safeguard personal data.

The advisory recommended several measures, including:

- Appointment of trained and certified Data Protection Officers;
- Conduct of Data Protection Impact Assessments (DPIAs);
- Deployment of Multi-Factor Authentication (MFA);
- Adoption of zero-trust security architectures;
- Continuous vulnerability management and patching;
- Cloud security enhancement;
- Real-time monitoring and threat detection systems;
- Encryption and secure credential management; and
- Regular Vulnerability Assessments and Penetration Testing (VAPT).

The advisory reflects the NDPC's growing emphasis on cybersecurity as a fundamental component of data protection compliance and highlights the increasing convergence between privacy governance and information security management.

Advisory Date

Issued

April 16, 2026

Target of threats

Nigeria's digital infrastructure and financial systems

Legal Basis

Obligations under the NDP Act for appropriate technical and organisational measures

NDPC and Meta Launch the Meta-Supported Initiative for Data Protection (M-SIDP)

On June 8, 2026, the NDPC launched the Meta-Supported Initiative for Data Protection (M-SIDP)[9], a two-year programme designed to strengthen Nigeria's data protection ecosystem.

The initiative emerged from a court-approved settlement reached after the NDPC investigated Meta's data processing practices in Nigeria. Under the settlement, Meta committed to supporting public-facing data protection programmes aligned with the objectives of the NDP Act, the General Application and Implementation Directive (GAID) 2025, and the NDPC Strategic Roadmap and Action Plan (SRAP) 2023 - 2027.

Programme duration

2 years

One of the most significant public-private collaborations in Nigeria's privacy ecosystem — reinforcing institutional capacity and public awareness on data protection issues.

Governance, research and policy development

Public-facing programmes aligned with the objectives of the NDP Act, GAID 2025 and SRAP 2023–2027.

Technology safety and sustainability

Support for a safer, more sustainable technology ecosystem for Nigerian data subjects.

Capacity building for DPOs and DPCOs

Strengthening Data Protection Officers and Data Protection Compliance Organisations.

Public awareness initiatives

Targeted at data subjects, particularly vulnerable groups.

The initiative represents one of the most significant public-private collaborations in Nigeria's privacy ecosystem. It reinforces the country's commitment to strengthening institutional capacity and public awareness on data protection issues.

CBN Introduces Enhanced Data Localisation Requirements for Fintech Operators

On June 15, 2026, the Central Bank of Nigeria (CBN) issued a circular introducing new compliance obligations for payment service providers, mobile money operators, and switching companies.[10] introducing new compliance obligations for payment service providers, mobile money operators, and switching companies. The circular mandates localising domestic transactional data within Nigeria and requires enhanced disclosure of Ultimate Beneficial Ownership (UBO) structures.

The framework aims to strengthen regulatory oversight, improve financial transparency, and support the protection of sensitive financial information. Non-compliant organisations face supervisory audits and regulatory sanctions.

The development is noteworthy from a data protection perspective, as it reflects a growing policy preference for local storage of critical datasets and closer scrutiny of cross-border data governance arrangements.

NDPC Issues Guidance on Continuous Professional Development Requirements for Data Protection Officers

On June 26, 2026, the NDPC released a **Guidance Notice** on Schedule 3 of the General Application and Implementation Directive (GAID) relating to Data Protection Officer (DPO) Assessment and Verification.

The guidance introduces a structured Continuous Professional Development (CPD) framework for certified DPOs, requiring annual participation in approved professional development activities as a condition for maintaining active verification status.

The framework establishes minimum CPD requirements covering:

Formal training and certification programmes

Knowledge contributions through publications and speaking engagements.

Participation in recognised professional and regulatory initiatives.

The guidance further demonstrates the Commission's efforts to professionalise the DPO function and promote the development of a globally competitive privacy workforce in Nigeria.

Nigeria's regulatory first half — at a glance

Feb 17
NDPC opens investigation into Temu's data processing practices

Apr 16
Data Protection Advisory on escalating cybersecurity threats

Jun 08
Launch of the Meta-Supported Initiative for Data Protection

Jun 15
CBN circular on data localisation for fintech operators

Jun 26
Guidance Notice on CPD requirements for DPOs

Updates from the European Union

February 11, 2026

EDPB & EDPS Joint Opinion on the Digital Omnibus Regulation

On February 11, 2026, the European Data Protection Board (EDPB), and European Data Protection Supervisor (EDPS) issued a Joint Opinion on the European Commission's proposal for a Digital Omnibus Regulation aimed at streamlining the EU's digital regulatory landscape and alleviating compliance obligations. The regulators welcomed some of the simplifications, but also expressed concerns that proposed new definitions of 'personal data' and how it should be treated in the GDPR, together with the treatment of pseudonymised data, might reduce the level of protection that would otherwise be available under the GDPR and the existing CJEU jurisprudence.

April 2026

Europrivacy certification scheme approved for international transfers

The Europrivacy certification scheme was approved by the EDPB in April 2026 as a suitable means of safeguarding for transfers to third countries under Article 46 GDPR. Organisations will have an extra transfer option in addition to SCCs and BCRs. It provides a harmonised approach to ensure sufficient level of protection for the transfer of personal data to jurisdictions with no adequacy decision.

April 14, 2026

Consultation on a standardised DPIA template

On April 14, 2026, the EDPB opened a consultation on a standardised DPIA template, with the aim of fostering the consistency of conducting and documenting DPIAs within the EEA. The proposed template includes description of processing activities, necessity and proportionality, risk assessment, risk mitigation and consultation with stakeholders as a means of fostering more accountability and aligning privacy risk assessments.

May – June 2026

Phased implementation of AI Act obligations

The European Commission invited the express acceleration of a solution for age verification in June 2026, based on privacy principles, which will enable persons to prove their age without disclosing their identity or exact age. It is a step taken by the EU to reconcile online child protection principles with the principles of data minimisation and privacy-by-design.

April 15, 2026

Guidelines 1/2026 on processing for scientific research

On April 15, 2026, the EDPB issued Guidelines 1/2026 on the Processing of personal data for scientific research, which cover among others the definition of the scientific research, purpose limitation, lawful bases, consent, special category data, and Article 89 safeguards. The Guidelines offer more clarity for research-intensive sectors and aim at promoting responsible science innovation without compromising due protection for data subjects.

June 2026

Accelerated solution for privacy-preserving age verification

EU institutions reached an agreement in May and June 2026 to delay some compliance deadlines for high-risk AI systems in order to allow more time to create technical standards and regulatory frameworks. Some high-risk AI obligations were put off, but important transparency obligations are still to be implemented from August 2026 – showing the ongoing alignment between AI governance and data protection compliance.

Contributors



Chidera Ezenwanne, ACArb
Senior Associate



Michael Arinze
Associate

Publications

01 Data Protection Outlook 2026

By **Nimma Jo-Madugu, Chidera Ezenwanne and Oluwapelumi Ikujenyo**

This paper reflects on Nigeria's data protection landscape for 2025 and offers a forward-looking assessment for 2026. It examines the regulatory, judicial, legislative, and market developments that will shape compliance and enforcement in 2026, including full enforcement of the General Data Protection Regulation (GDPR) 2025, Open Banking implementation and data governance, Litigation/Dispute trends, international data transfer, and Global integration.

This paper can be accessed here: **KENNA.**

02 Data Protection Annual Audit Returns in Nigeria

By **Eunice Alasa, Michael Arinze and Adesuwa Akhigbe**

This paper addresses the requirements for Data Protection Annual Audit Returns in Nigeria. It highlights key issues controllers and processors must address to avoid regulatory exposure and reputational risk. It highlights the requirement to file annual Compliance Audit Returns (CAR), as stipulated under the National Data Protection Commission's (NDPC) General Application and Implementation Directive (GAID) 2025. The paper provides the systems and structures to be implemented by data controllers and processors to ensure defensible Annual Audit Returns.

This paper can be accessed here: **KENNA.**

03 Data Processing Agreements Under the NDP Act 2023

By **Nimma Jo-Madugu, Chidera Mbaogu and Michael Arinze**

This paper examines the legal foundation of Data Processing Agreements (DPAs) in Nigeria. It emphasises their role in defining the rules for sharing, processing, and securing personal data between a data controller and a data processor. It clearly explains the mandatory contents of a DPA under the General Application and Implementation Directive (GAID) 2025. It highlights the legal and compliance implications of failing to execute a DPA.

This paper can be accessed here: **KENNA.**

04 After the Breach: Legal Strategies for Response, Recovery, & Resilience

By **Okechukwu Ekweanya, Sonia Onyia and Okenna Onyelu**

This paper outlines the required procedures for responding to data breaches under the Nigeria Data Protection Act (NDPA) 2023 and the General Application and Implementation Directive (GAID) 2025. It examines the statutory reporting threshold for data breaches, preventive measures to safeguard data, and the need for organisations to implement privacy pillars as a proactive step in governance and data breach prevention.

This paper can be accessed here: **KENNA.**

Contributors



Oluwapelumi Ikujenyo
Associate



Favour Adeniyi
Associate

Key Contacts



Nimma Jo-Madugu, CIPP/E
Partner



Oluwapelumi Ikujenyo
Associate

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

Endnotes

1. (2026) EWCA CIV 140
2. Suit No: FHC/ABJ/CS/1181/2025
3. Sui No: LD/19478MFHR/2025
4. SUIT NO: LD/17783MFHR/2025
5. [2026] EWCA CIV 140
6. RECORD NO: 2025/248 MCA
7. https://punchng.com/ndpc-probes-e-commerce-platform-temu-over-data-breach/ Accessed October 27, 2026
8. https://punchng.com/ndpc-raises-the-alarm-over-cyberattacks-on-nigerias-financial-systems/ Accessed October 27, 2026
9. https://punchng.com/ndpc-probes-e-commerce-platform-temu-over-data-breach/ Accessed October 27, 2026
10. Circular No. PSS/DIR/PUB/CIR/001/004



CONTACT

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 | www.kennalp.com