



DATA PROTECTION

Newsletter



P a g e s

C O N T E N T S

2

Introduction

5

From the Court

10

Data Breach Watch

12

Regulatory Updates

19

Publications

Introduction

The Nigerian data protection sector has continued its path of resilient and encouraging growth nationwide. The first half of 2025 recorded important developments, emphasizing Nigeria's sustained commitment towards protecting digital rights and, in the broader context, building a more inclusive and secure digital ecosystem. Now in its sophomore year, the Nigerian Data Protection Commission (NDPC) has intensified its efforts to give full effect to the provisions of the *Nigerian Data Protection Act (NDPA)*, primarily through policies and frameworks, including the introduction of the *General Application and Implementation Directive (GAID)*.

The *GAID*, as an implementation framework, contextualizes the provisions of the *NDPA* with the aim of improving both understanding and compliance in practice. These efforts have had a ripple effect on the economy, particularly in expanding the scope and quality of data compliance services currently available. It is not surprising that the sector is projected to generate around N13 billion in revenue for the year.¹

Interestingly, however, the most noteworthy policy shifts in the year have come from judicial pronouncements. Landmark judicial decisions, like the cases of *Araka v E-Cart Internet Services Limited & Anor.*² and *The Incorporated Trustees of Personal Data Protection Awareness Initiative v Nizamiye Hospital Limited*,³ have not only set important precedents for the future but have also accentuated the enforceability of the *NDPA*. These cases reflect an increasing awareness among data subjects of their rights and the willingness to enforce these rights through the necessary legal channels. They also contribute to the growing body of data protection jurisprudence in Nigeria, complementing the existing regulatory policies.

Additionally, countries around the globe are not left out; several regulatory trends have defined the global data protection narrative. For example, the Digital Operational Resilience Act (DORA), applicable to European Union states, became effective on January 17, 2025. Like, several US states implemented new privacy laws in 2025, expanding data protection requirements.

1 Balogun F, 'Nigeria Targets N13.8bn from Data Protection in 2025' (*Businessday NG*, 25 April 2025) <<https://businessday.ng/technology/article/nigeria-targets-n13-8bn-from-data-protection-in-2025/>> accessed 3 July 2025

2 FHC/ABJ/CS/195/2024

3 FCT/HC/GAR/CV/187/2024. Notably referred to as *ITPDPAI v Nizamiye*



Notwithstanding regulatory efforts, data breaches continue to occur on a significant scale. In one instance, cybersecurity firm Surfshark released a report detailing that more than 119,000 data breaches had been recorded in Nigeria in the first quarter of 2025.⁴ Clearly, while progress has been made, much work remains to be done to ensure adequate protection.

In this newsletter, we delve into some of the recent developments in the data protection landscape, we feature key regulatory and enforcement updates from Nigeria and across the globe, and we shall also highlight notable court decisions which are gradually shaping the Nigerian data protection jurisprudence.

4 Akintaro S, 'Nigeria Records 119,000 Data Breaches in Q1 2025, Ranks 34th Globally –Report' (*Nairametrics*, 10 May 2025) <<https://nairametrics.com/2025/05/10/nigeria-records-119000-data-breaches-in-q1-2025-ranks-34th-globally-report/>> accessed 3 July 2025.



From the Court

Republic v Tools for Humanity Corporation (US) & 8 others; Katiba Institute & 4 others (Ex parte Applicants); Data Privacy & Governance Society of Kenya (Interested Party) (Judicial Review Application E119 of 2023) [2025] KEHC 5629 (KLR)

The Applicants, the Katiba Institute & 5 Ors., instituted an action against the 1st – 9th Respondents,⁵ including, Tools for Humanity Corporation (US) and the Central Bank of Kenya, alleging that they violated the constitutional rights to privacy under Article 31 of the Kenyan Constitution and provisions of the Kenya Data Protection Act of 2019 (the Act) by:

- i. collecting and processing iris and facial scans from Kenyan residents without conducting an adequate Data Protection Impact Assessment (DPIA);
- ii. processing data without valid consent, since data subjects were offered cryptocurrency tokens in exchange for their biometric data; and
- iii. transferring personal data across borders without sufficient legal safeguards.

On May 5, 2025, Honourable Justice Roselyne Aburili decided that Tools for Humanity Corporation (US) and the other parties violated Section 31 of the Kenya's Data Protection Act by collecting and processing biometric data—iris and facial scans—without a proper Data Protection Impact Assessment (DPIA), valid consent, or adequate cross-border safeguards. The Court held that the consent obtained was not genuine or lawful because it was induced by offering cryptocurrency, and was not freely given, informed, or specific, in violation of Sections 2 and 30 of the Act. The Court also found them liable for transferring biometric data to foreign jurisdictions without demonstrating that sufficient safeguards were in place.⁶

Accordingly, the Court issued an order of injunction prohibiting all collection, processing, or transfer of the personal biometric data collected in Kenya, without undertaking or conducting a data protection impact assessment in accordance to section 31 of the Act or using consent obtained through inducement of a cryptocurrency — Worldcoin. The Court also

5 One trust, Data Guidance "Kenya: High Court orders Worldcoin entities to stop collection and processing of biometric data" (One trust, data guidance, May 8 2025) < <https://www.dataguidance.com/news/kenya-high-court-orders-worldcoin-entities-stop> > accessed July 24, 2025.

6 Republic v Tools for Humanity Corporation (US) & 8 others; Katiba Institute & 4 others (Ex parte Applicants); Data Privacy & Governance Society of Kenya (Interested Party) (Judicial Review Application E119 of 2023) [2025] KEHC 5629 (KLR) (Judicial Review) (5 May 2025) (Judgment) <<https://new.kenyalaw.org/akn/ke/judgment/kehc/2025/5629/eng@2025-05-05>> accessed July 24, 2025.

ordered that all unlawfully collected biometric data be deleted within 7 days, under the supervision of the Office of the Data Protection Commissioner. Additionally, the Court quashed all prior administrative permissions or acts that purported to authorize such activities in Kenya.⁷

This ruling underscores the importance of ethical data practices, especially in emerging technologies, and serves as a warning to tech companies operating in Africa to comply strictly with local data protection laws.

The Incorporated Trustees of Personal Data Protection Awareness Initiative v Nizamiye Hospital Limited⁸

In the landmark case of *Incorporated Trustees of Personal Data Protection Awareness Initiative (PDPA) v. Nizamiye Hospital*,⁹ the data protection obligations of a data controller and the enforcement mechanisms for these obligations were critically examined. PDPA alleged that the Hospital installed a CCTV surveillance and website tracking device without appropriate disclosure and notification to the data subjects. They also claimed that the hospital failed to conduct a data privacy impact assessment (DPIA) and deploy privacy notices on its website and other data collection medium to inform data subjects of how personal their data is collected, processed, and stored.

In this dispute, the key issues for determination before the Honourable court were as follows:

- i. Whether the Personal Data Protection Awareness Initiative (PDPA) has locus standi to institute and prosecute the suit as a public interest group;
- ii. Whether the facts constitute a cause of action against the Hospital; and
- iii. Whether the facts constitute a breach of privacy under the Nigerian Data Protection Act (NDPA) 2023.

On April 10, 2025, the Court held that the PDPA possessed the requisite *locus standi* to institute and prosecute the matter, on behalf of data subjects, thereby affirming the suit's status as public interest litigation. The Court, however, decided that there is no substantive proof of a breach

⁷ Ibid

⁸ FCT/HC/GAR/CV/187/2024 (Unreported). Notably referred to as *ITPDPAI v Nizamiye*.

⁹ Ibid

of privacy under the Nigerian Data Protection Act 2023, as the CCTV monitoring in question was for the benefit of the public in terms of safety.¹⁰ This constitutes an exception to the requirement for consent under the Act.

This decision of the Court provided clarity on whether an NGO could institute an action for the enforcement of data subjects' rights on their behalf, as well as under what circumstances an allegation of breach of data privacy would be unsuccessful.

*Araka v E-Cart Internet Services Limited & Anor.*¹¹

In this matter, Chukwunweike Akosa Araka (**the Applicant**), a regular user of the now-defunct Jumia Food app (Jumia Food) operated by E-cart Internet Services (**1st Defendant**), placed several food orders from Domino's Pizza (operated by Eat 'N' Go Limited, the **2nd Defendant**) through the app in March 2023. Jumia Food required users to submit personal data, such as phone numbers and addresses, to facilitate deliveries. Although Araka never directly shared his contact details, he received unsolicited promotional messages from Eat 'N' Go about seven months later. In line with his rights under the NDPA, Araka requested that Domino's desist from processing his personal data for promotional marketing purposes.

In response, Domino's stated that the data was processed lawfully, fairly, and for legitimate business purposes. They argued that having received the Araka's objection in early 2024, they had interpreted the message as a request for deletion and removed his details from their database. However, when he placed a new food order through a different app, Glovo, in March 2024, he re-established a business relationship, and the lawful basis of Araka's consent was renewed. Based on this, they contended that the resumption of marketing messages was lawful, as the new transaction provided a fresh legal basis for processing and using his data for communication, including promotional messaging.

In its judgment, the Federal High Court held that the Eat 'N' Go had no legal basis under Nigerian law to continue sending promotional messages

10 Precious Onuabuchi, 'Data, Consent, and Public Interest within The Legal Boundaries Of Data Privacy: The case of PDPA V. NIZAMIYE HOSPITAL' (Business Day, May 29, 2025) < <https://businessday.ng/news/legal-business/article/data-consent-and-public-interest-within-the-legal-boundaries-of-data-privacy-the-case-of-pdpa-v-nizamiye-hospital> > accessed July 4, 2025.

11 FHC/ABJ/CS/195/2024 : Araka v E-Cart Internet Services Limited & Anor

after the Araka's objection. The Court further noted that the continued processing of his data for marketing purposes was a violation of data protection laws and that placing his food order via a different platform did not constitute a valid justification for reviving previously revoked consent, thus reaffirming data subjects' rights to control how their personal data is used. Accordingly, the Court entered judgment in Araka's favour and fined the Eat 'N' Go to the tune of N3,000,000.00 (Three Million Naira Only).¹²

The Court's decision reaffirmed the rights of data subjects to control how their personal data is used, as well as a caution to data processors and controllers that when consent is given, the data must only be used for the purpose for which consent was given.

12 BD Law Digest with CLRN and ALP NG & Co, 'Data processing is deemed lawful only when it is necessary for fulfilling a contract in which the data subject is a party' (*Business Day*, April 10, 2025) < <https://businessday.ng/news/legal-business/article/data-processing-is-deemed-lawful-only-when-it-is-necessary-for-fulfilling-a-contract-in-which-the-data-subject-is-a-party/> > accessed July 3, 2025.



Data Breach Watch

16 billion passwords leaked in a major global data breach

On June 18, 2025, Cybernews researchers reported the discovery of 30 unsecured datasets containing over 16 billion records.¹³ The data included everything from private citizen logins to accounts tied to government domains, as well as passwords and social media accounts, including Facebook, Telegram, Instagram, and PayPal.¹⁴

Widely considered the largest password leak in history, it reportedly involved the exposure of over 16 billion passwords belonging to users worldwide.¹⁵ This leak is particularly alarming because it is not tied to a specific breach of one organization, but rather a collection of compromised credentials from various sources, making it a significant threat to both individuals and organizations.

As a necessary safeguard, it is highly recommended that users change all their account passwords or, at least, those credentials that have been reused across multiple services. You can also verify if your email account has been compromised [here](#).

13 Sayegh E, 'Silent Breach Exposes 16 Billion Passwords: 5 Things You Must Do Now' (*Forbes*) < <https://www.forbes.com/sites/emilsayegh/2025/06/30/silent-breach-exposes-16-billion-passwords-5-things-you-must-do-now/> > accessed 3 July 2025

14 Ibid

15 Online | ET, '16 Billion Passwords Leaked! The Biggest Data Breach Ever? | TechPulse' (*The Economic Times*, 30 June 2025) < <https://economictimes.indiatimes.com/tech/technology/16-billion-passwords-leaked-the-biggest-data-breach-ever-techpulse/videoshow/122162810.cms> > accessed 3 July 2025



Regulatory Updates

NDPC GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVE (GAID) 2025

In March 2025, the Nigerian Data Protection Commission (NDPC) issued the General Application and Implementation Directive (GAID). This directive replaces the Nigeria Data Protection Regulation (NDPR) 2019 as the primary instrument regulating data protection in Nigeria under the Nigeria Data Protection Act (NDPA) 2023.

Key Highlights:

1. **Repeal of NDPR 2019:** The GAID supersedes the NDPR as the principal regulatory framework for data protection. However, actions taken under the NDPR prior to the issuance of the GAID remain valid and enforceable.
2. **Clarification on the Role of Data Protection Officers (DPOs):** Organisations subject to the NDPA must appoint a Data Protection Officer, who may be an internal staff member or an external service provider, in line with Section 32 of the NDPA.
3. **Introduction of Legitimate Interest Assessment (LIA):** Data Controllers/Data Processors (DC/DPs) must now conduct a Legitimate Interest Assessment (LIA) before engaging in data processing activities that rely on legitimate interest as a legal basis. A standard template is included in the GA.

This directive represents a significant milestone in Nigeria's data protection evolution, providing clarity, structure, and alignment with global best practices. Organisations are advised to review their data governance frameworks and ensure full compliance with the new requirements.

DATA PROTECTION IMPLICATIONS IN THE OPEN BANKING LAW IN NIGERIA

Open banking is a system that enables banks and other financial institutions to securely share customers' financial data with Third-Party Providers (TPPs)

through electronic means. It essentially involves making customer data available to each other and to qualified third parties through standardized Application Programming Interfaces (APIs). The technical backbone of open banking is built on APIs, software intermediaries that allow different applications to communicate and exchange data seamlessly.

Under this framework, banks provide authorized TPPs such as fintech companies and other regulated financial innovators access to customer transaction data via secure APIs. This access empowers TPPs to develop new, tailored financial products and services, fostering innovation, improving customer experience, and advancing financial inclusion.

The sharing of financial data which is central to the operation of open banking presents significant opportunities for innovation and financial inclusion. However, it also introduces heightened risks, particularly concerning data privacy and security. As customer data is shared across multiple platforms and third-party service providers, the potential for unauthorized access, misuse, or data breaches increases. This expanded data ecosystem amplifies the vulnerability of sensitive financial information, thereby necessitating robust regulatory safeguards.

In February 2021, the Central Bank of Nigeria (CBN), exercising its statutory authority as the regulator of the Nigerian banking sector, introduced the *Regulatory Framework for Open Banking in Nigeria*.¹⁶ Building on this foundation, the CBN further strengthened its regulatory oversight of open banking by issuing the Operational Guidelines for Open Banking in Nigeria¹⁷ on March 7, 2023, providing detailed guidance on implementation and compliance.

The Regulatory Framework for Open Banking in Nigeria has established principles for data sharing across the banking and payments system to promote innovations, drive competition, improve accessibility to financial and payments services and broaden the range of financial products and services available to bank customers. Participants in open banking are required to adhere strictly to security standards when accessing and storing data, and are subject to minimum privacy, operational, customer experience and risk management standards.

16 Regulatory Framework for Open Banking in Nigeria, available at <https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf>, accessed on July 23, 2025

17 Operational Guidelines for Open Banking in Nigeria, available at <https://www.cbn.gov.ng/Out/2023/CCD/Operational%20Guidelines%20for%20Open%20Banking%20in%20Nigeria.pdf> accessed on July 23, 2025.

Guideline 9.2 of the CBN Guidelines explicitly provides: “APs/ACs¹⁸ shall comply with the Nigerian Data Protection Regulation¹⁹ or any CBN-issued data protection regulation for financial institutions, to protect customer data.” This underscores the requirement that all participants in the open banking ecosystem must adhere to applicable data protection laws and regulations.

Flowing from the above, several key provisions of the NDPA have direct implications for open banking and the handling of personal financial data:

a. *Provision of Information to the Data Subject*

Section 27 of the NDPA requires that before collecting personal data, a data controller must provide the data subject with specific information, including: the identity, residence, and place of business of the data controller; the purpose of the processing; the retention period for the data; and the rights of the data subject, including the right to lodge a complaint with the Nigeria Data Protection Commission (NDPC).

This requirement is particularly relevant in open banking, where banks acting as data controllers often possess significant informational advantage over customers. Transparent disclosure ensures that customers are fully informed about how their data will be shared with third parties and the implications of such sharing.

b. *Rights of the Data Subject*

Section 34 of the NDPA enumerates the rights of data subjects, including: the right to object to the processing of their personal data, the right to withdraw consent at any time, the right to access, correct, or erase their data; and the right to data portability.

These rights are significant in the context of open banking, where some individuals may be reluctant to share their financial information with third parties. The law ensures that such individuals have the right to object to processing and to withdraw consent without incurring any cost or facing undue barriers.

¹⁸ API Providers and API Consumers (API: Application Programming Interface).

¹⁹ The NDPR has now been replaced by the NDPA

c. Data Security Obligations

Section 39 of the NDPA requires data controllers and data processors to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in their possession or under their control, including protections against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure, or access, considering, some important guidelines.

Furthermore, Section 40 of the NDPA imposes a duty to report data breaches on data processors. That is, where a data processor becomes aware of a personal data breach, it must immediately notify the data controller that engaged it; and provide all necessary information to enable the data controller to respond to and resolve the breach in accordance with the law.

Companies and Institutions (The data processor) that have obtained the financial information of customers through open banking are legally obligated to inform banks (the data controller) if a breach occurs and cooperate in mitigating the incident.

d. Requirement for Valid Consent

Consent is a foundational principle of lawful data processing under both the NDPA and the CBN Guidelines. **Guideline 7.0** of the CBN Guidelines mandates that explicit consent must be required from customers whose data are required to avail them open banking products and services. Under Section 26 of the NDPA, consent must be freely given; specific, informed, unambiguous and given through clear affirmative action. Critically, the burden of proof lies with the data controller to demonstrate that valid consent was obtained. This places a high compliance obligation on banks and third-party providers to maintain auditable records of consent.

e. Penalties for Non-Compliance

Section 48 and 49 of the NDPA provides for strict penalties for breaches of data protection obligations. Any person or entity found to have violated the rights of a data subject may be liable to administrative fines, sanctions, or other enforcement actions by the NDPC. Also, a data subject who suffers

injury, loss or harm as a result of the violation of the Act by a data controller or data processor may be allowed to recover damages from such data controller or data processor.²⁰

Given the increased exposure to data risks in open banking environments, all participants, banks, fintechs, and API providers must ensure strict compliance with both the CBN Guidelines and the NDPA to avoid regulatory sanctions and reputational harm.

The CBN Guidelines, when read in conjunction with the NDPA, create a comprehensive regulatory framework that strikes a balance between innovation and accountability. Stakeholders must prioritize transparency, security, and respect for data subject rights to ensure the sustainable and lawful development of open banking in Nigeria.

**TABLE OF DATA PROTECTION REGULATORY
UPDATES ON A GLOBAL SCALE**

Country	Regulation	Regulatory Update
United Kingdom	The Data (Use and Access) Act 2025	This is a wide-ranging Act which includes provisions to enable the growth of digital verification services, new Smart Data schemes like Open Banking and a new National Underground Asset Register. It also includes some important changes to the UK's data protection and privacy legislation.
United States of America	American Privacy Rights Act (APRA)	This is a comprehensive data privacy law proposed in the United States. It would place limitations on the kinds of data companies can collect about their users, create processes for users to access or remove data about themselves, and allow users to opt out of having their data sold by data brokers.

20 Section 51 of the Nigeria Data Protection Act, 2023

Canada	Consumer Privacy Protection Act (CPPA)	This is a modernization of Canada's existing data privacy regulations. Similar to the GDPR, the CPPA (Bill C-11) applies to any organization that processes the personal data of Canadian citizens for commercial purposes, regardless of where they are located. The CPPA is designed to replace the existing Personal Information Protection and Electronic Documents Act (PIPEDA). It gives consumers elevated rights when it comes to pursuing legal action against companies who fail to adequately protect the confidentiality of their data.
Singapore	Personal Data Protection (Amendment) Act 2024	This introduces several key changes to the existing Personal Data Protection Act 2010 (PDPA). These changes include the mandatory appointment of a Data Protection Officer (DPO) under specific circumstances, enhanced penalties for non-compliance, and the extension of the security principle to data processors. The Act also addresses the handling of personal data breaches and introduces the concept of data portability for data subjects.
India	Digital Personal Data Protection Act (DPDPA), 2023	This is a landmark Indian law aimed at safeguarding individuals' digital personal data and regulating its processing. It establishes a framework for data protection, balancing individual rights with the legitimate needs of businesses and other organizations. The Act emphasizes consent, data minimization, and the right to be forgotten, while also imposing obligations on data controllers and processors to ensure data security.



Publications

The Right to Erasure: An Overview of the Judgment of the Federal High Court in *Olatokun v Polaris Bank* (Suit No: LD/17392MFHR/2024) Vis-a-Vis the Rights of a Data Subject

by *Eunice Alasa, Chidera Ezenwanne and Oluwapelumi Ikujenyo*

The paper examines the right to erasure under Nigeria's Data Protection Act 2023, using the case of *Tokunbo Olatokun v Polaris Bank* as a focal point. It highlights how the Court upheld the data subject's right to privacy and erasure when the bank failed to stop processing his data after a clear request. The judgment reinforces the enforceability of data protection rights in Nigeria. The paper stresses the need for stronger regulatory enforcement and organisational compliance. Overall, it sets a precedent for striking a balance between digital innovation and privacy rights in Nigeria.

This paper can be accessed here [KENNA](#)

Frank Ijege v NDPC (Suit No. FHC/KD/CS/34/2024): Effect of the Judgment of the Federal High Court on the NDPC 2023 Guidance Notice

by *Nimma Jo-Madugu, Chidera Ezenwanne, Oluwapelumi Ikujenyo and Michael Odozi*

The paper examines the legal implications of the Federal High Court's Judgment on the rights of data subjects' vis-a-vis the NDPC 2023 Guidance Notice using the case of *Frank Ijege v NDPC* as a focal point. This case essentially examined the legality of the Commission's Guidance Notice issued in 2024 on the registration of data controllers and data processors of major importance ("the Guidance Notice" or "the Notice"). The judgment of the Court has legal implications for Nigeria's data protection landscape, emphasising the need for regulatory actions to align strictly with statutory provisions to avoid an overreach.

This paper can be accessed here [KENNA](#).

Frequently Asked Questions Regarding the Nigeria Data Protection Act (NDP Act) 2023: General Application and Implementation Directive (GAID)

by Chidera Ezenwanne, Oluwatobi Sanni, Jessica Obodo-Elue

The FAQ outlines key provisions of the Nigeria Data Protection Act (NDP Act) 2023 and the General Application and Implementation Directive (GAID), serving as a guide for data controllers, processors, and individuals. It explains compliance duties such as registration, audit filing, data breach notifications, and appointment of Data Protection Officers (DPOs). The document clarifies the rights of data subjects and obligations of data controllers or data processors such as privacy policies, cookie use, and internal data protection schedules.

Enforcement Of the Rights of a Data Subject – Practicability Under the Nigerian Data Protection Act 2023 (NDP Act) and The General Application and Implementation Directive (GAID) 2025

by Chidera Ezenwanne, Oluwatobi Sanni, Jessica Obodo-Elue

The article analyzes the legal framework for protecting and enforcing data subjects' rights under the NDPA 2023 and GAID 2025. It highlights the broad rights granted to individuals, including access, correction, erasure, and restriction of processing. The GAID complements the Act by outlining detailed complaint procedures and introducing tools like SNAG for internal resolution.

Frequently Asked Questions Regarding Data Protection Compliance in Nigeria

This paper highlights answers critical questions on data protection in Nigeria using the NDPA as a focal point. NDPA governs the processing of personal and sensitive data, including identifiable and pseudonymized information. It grants data subjects' rights like access, correction, and erasure, though these rights are not absolute. All organisations operating in or targeting Nigeria must comply, including foreign companies. Non-compliance attracts heavy fines, possible legal action, and regulatory penalties.

This paper can be accessed here [KENNA](#).



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

3 Emmanuel Ngwu Street,
Thinkers' Corner,
Enugu, 400001

+234 811 395 1052, +234 811 395 1053
ealasa@kennapartners.com
qadeoye@kennapartners.com
counsel@kennapartners.com

