Privacy Digest

Issue 2 | February 2025

KPMG in Nigeria

Collect Only the Data You Need, for the Right Purpose

As the amount of personal data collected and processed by organisations continues to increase, the need for responsible data processing is paramount. Among the core principles guiding responsible data protection are Data Minimisation and Purpose Limitation. These foundational principles embedded in the NDPA, play crucial roles in shaping how data is collected and processed by organisations. They emphasise that data controllers/processors must be accountable for data collected and ensure that personal data is:

- "collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes" (*See NDPA Section 24 (1)(b) – Purpose Limitation*);"
- "adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed" (*See NDPA Section 24(1) (c) – Data Minimisation*)."

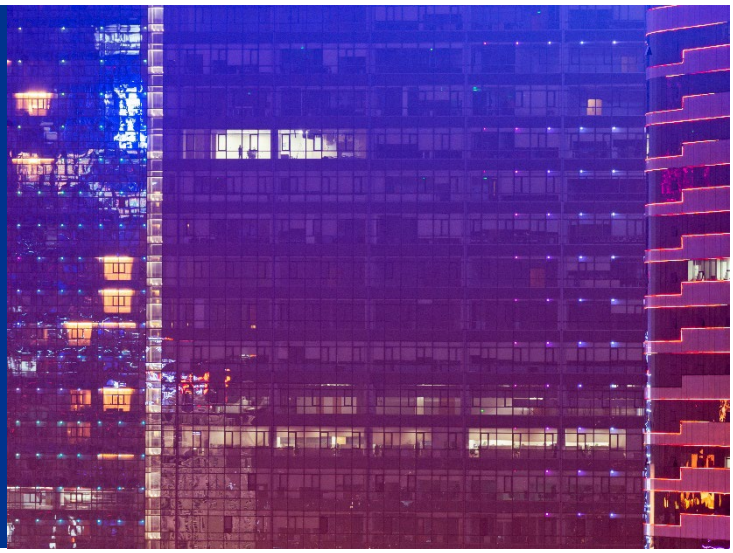
While the NDPA is more recent, other prominent privacy regulations such as the EU GDPR also reference similar requirements for Data Minimisation and Purpose Limitation. Compliance with these requirements will require understanding and evaluation of existing data collection and processing activities across an organisation.

In this edition, we will discuss the concepts of Data Minimisation and Purpose Limitation, as well as the provisions of the Nigeria Data Protection Act (NDPA) and other prominent privacy laws on this subject.
We will explore examples of Data Minimisation and Purpose Limitation in action, case studies on the correct vs incorrect ways to implement the principles of Data Minimisation and Purpose Limitation, lawful basis in relation to Data Minimisation and Purpose Limitation, enforcement fines relating to Data Minimisation and Purpose Limitation across the globe, emerging trends influencing these concepts, among others.

Less is More

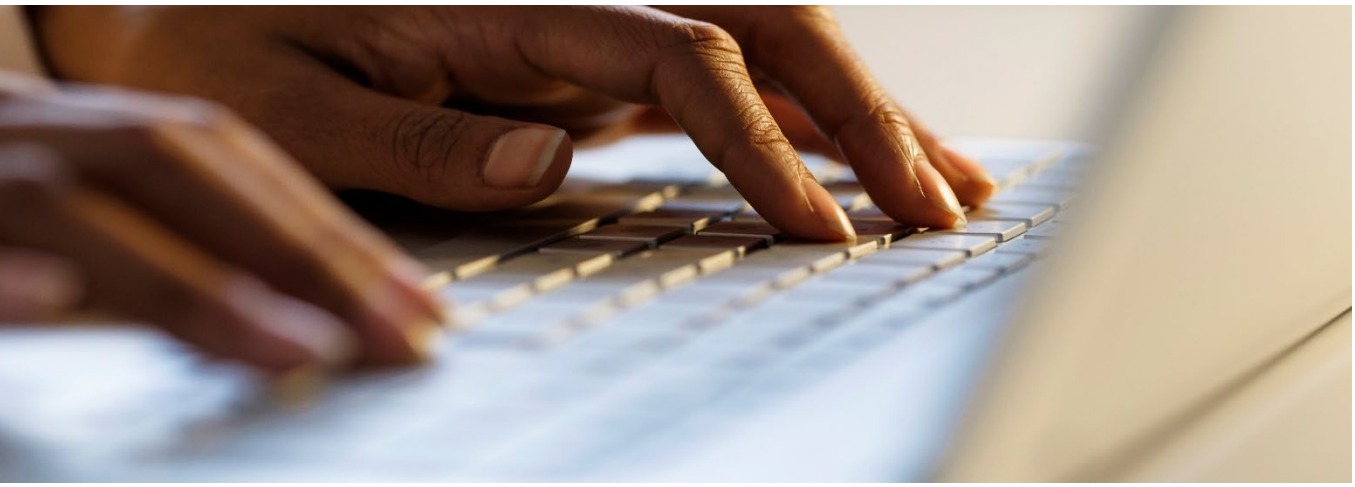
As earlier stated, Data Minimisation is a key principle enshrined in the Nigeria Data Protection Act (NDPA). This principle is designed to ensure that organisations handle personal data with utmost care by collecting only the information necessary for their specific purposes. The goal is to protect individuals' privacy and reduce the risks associated with over-collection, misuse, or unintended exposure of personal data. By adhering to the Data Minimisation principle, organisations contribute to a more secure and compliant data handling environment, in line with NDPA's overarching aim to safeguard personal data in Nigeria.

Next is a case study to provide perspectives on how this principle is applied in practice.



Case Study 1

Consider a Nigerian e-commerce company that requires personal information to process orders and deliver products to its customers. According to NDPA's principle of Data Minimisation, the company should only collect the information that is essential for processing the transaction. This may include the customer's name, phone number, delivery address, and payment details. The company should avoid requesting additional personal information, such as the customer's Bank Verification Number (BVN), information about other members of the customers' family or detailed demographic data unless the company has a lawful basis for processing this information relative to the business transaction. Furthermore, after the order is fulfilled and any necessary post-transaction communications are completed, the company should securely delete the data that is no longer required in accordance with its data retention schedule. This approach aligns with the NDPA's emphasis on collecting only what is necessary and retaining data only for as long as necessary to fulfill its intended purpose.



Using Data in the Right Manner

Purpose limitation ensures that data is used strictly for the reason it was collected, preventing mission creep where personal information is repurposed for unrelated or secondary objectives. Complying with the principle of Data Minimisation enables organisations to reduce the probability of violating the principle of Purpose Limitation. When organisations collect only the necessary amount of data to achieve a specific goal, it restricts the use of data to only what has been obtained. However, this does not imply that the limited data obtained cannot be repurposed to achieve other objectives incompatible with the original purpose. Hence, organisations must recognize that minimising data collection is not sufficient. They must align the usage of the data collected with the exact purpose for which it is intended and not repurpose the minimized data collected for a different use, unless the further processing is compatible with the originally specified and legitimate purpose for which it was collected.

Using Case Study 1, we will illustrate how Data Minimisation could inform Purpose Limitation. The e-commerce company collects and uses the personal data solely for processing orders and ensuring delivery. By collecting only the necessary personal data that is required - such as name, phone number and delivery address - the principle of Data Minimisation has ensured only essential personal data is collected. However, the principle of Purpose Limitation connotes that the use of the collected personal data should be restricted to the originally intended objective for the data collection. The company must ensure that every data point collected aligns directly with the purpose of fulfilling the order, thereby preventing repurposing of the data to fulfil a different objective. This practice aligns with the NDPA's requirement to ensure that personal data is only used in ways that are consistent with the purposes for which it was collected.

Are You Really Being Proactive, Or...?

It is not uncommon for some organisations to take a proactive stance by requesting data from data subjects for purposes not immediately required but possibly envisaged. In some of these instances, the data subject may eventually not qualify for such intended processing activity or may not take an action that will warrant such processing activity.

For instance, in the case study above, requesting a user's home address during account creation on the e-commerce platform may violate the principle of Data Minimisation, as this information is not essential at that stage. However, collecting the delivery address at the checkout stage aligns with Data Minimisation, as the personal data is necessary to fulfil the order.

Hence, it is important to note that the point at which personal data is collected plays a crucial role in ensuring compliance with data protection principles.

Lawful Basis in relation to Data Minimisation and Purpose Limitation

The importance of defining a lawful basis in data collection and processing

The Nigeria Data Protection Act (NDPA) 2023 outlines lawful bases for data processing under Section 24(1), specifying the conditions under which personal data processing is considered lawful. These lawful bases include consent, the performance of a contract, compliance with legal obligations, the protection of vital interests, public interest, and legitimate interests. Defining a lawful basis for data collection is crucial in upholding the principles of Data Minimisation and Purpose Limitation, as it establishes a clear justification for the collection and usage of personal data. When a lawful basis is properly identified, it guides the specific types and volume of data that can be collected, ensuring that only what is necessary for a legitimate purpose is processed.

The role of Data Minimisation and Purpose Limitation in Compliance to Lawful Basis

It is important to note that an organisation can comply with Data Minimisation and Purpose Limitation principle from the onset, but as business objectives evolve, new ways of maximising the use of the data may emerge. However, the organisation should not simply repurpose the data just because an original purpose of collection exists. The organisation must recognize the shift in purpose and reassess the lawful basis for the new processing, as the initial lawful basis may no longer apply for such further processing. Ensuring compliance with Purpose Limitation requires aligning any new data use with an appropriate lawful basis before proceeding. Using Case Study 1 as an example, we will illustrate how Data Minimisation and Purpose Limitation guides compliance with a lawful basis.

Initial Purpose - The company collects and uses the data solely for processing orders and ensuring delivery.

Restricted Use - The company should not use this data for unrelated purposes, such as sending marketing materials, without relying on a lawful basis for such processing activity.

Further Processing - If the company wants to use the data for a new purpose, such as for targeted ads or conducting market research, it must ensure that this new use is compatible with the original purpose and not use the data for a different purpose without relying on a justifiable legal basis for such subsequent processing. By aligning processing activities with these principles, organisations not only comply with the NDPA but also foster trust with data subjects by demonstrating respect for their privacy rights.

Advantages of Data Minimisation and Purpose Limitation

Adopting the principles of Data Minimisation and Purpose Limitation provides significant benefits for organisations. By limiting the data collected and defining clear purposes for its use, organisations can reduce risks, lower costs, and foster stronger customer relationships. Some key advantages include:

- **Reduces cost:** Data minimisation allows your organisation to collect, store and process only the data your organisation needs. Less expenditure on data collection and storage leads to more savings.

- **Facilitates adherence to data privacy regulations such as the NDPA:** The Act requires organisations that hold personal data to apply Data Minimisation policies to protect data; by complying with these regulations, organisations avoid legal penalties and build a positive reputation for respecting privacy rights. Infringements of NDPA provisions can lead to fines up to N10,000,000, and 2% of an organisation's annual gross revenue in the preceding financial year.

- **Faster Response to Data Subject Requests:** Under section 34 of the NDPA, data subjects have several rights that data controllers and data processors are obligated to fulfil. With fewer data to work with, organisations can respond promptly to data requests from consumers and avoid legal problems.

- **Customer trust and loyalty:** When individuals have confidence that their personal data will only be used for specified purposes, they are more likely to trust the organisation with their information. This trust fosters stronger relationships and promotes customer loyalty.

- **Facilitating a clear understanding of data usage:** Purpose limitation requires organisations to clearly specify the purposes for which they collect and process personal data. This clarity helps individuals understand exactly how their data will be used before they give consent. For instance, when consenting to receive marketing emails, individuals know precisely what type of communication they are agreeing to receive.

- **Prevention of unauthorised processing:** Purpose Limitation acts as a safeguard against unauthorised or unlawful processing of personal data. Any deviation from the initially stated purposes without a legal basis is considered a breach of NDPA, reinforcing the protection of individuals' rights.

Striking the Balance: Minimizing Data Collection and Defining Clear Purposes in Privacy Statements

Privacy statements can encompass various documents that inform users about data practices, including privacy notices, cookie notices, etc. These statements are designed to provide transparency, outlining what personal data is collected, how personal data is used, and protected. Regardless of the format, they all serve the same purpose: to ensure users are informed and their privacy rights are respected.

Below are examples of common mistakes in privacy statements frequently used by organisations and some model examples below:

1. Marketing Data Collection

✗ **Broad Purpose:** "We collect data to improve our business operations."
Issue: This purpose is too vague. It doesn't specify what data will be used for certain aspects of business improvement. It lacks clarity on the scope and use of the data, which can lead to misuse or non-compliance with the NDPA.

✓ **Specific Purpose:** "We require your email address to send you our monthly newsletter about product updates and promotions."
Advantage: This purpose is clear and specific. It explicitly states what data is required and collected (email address), how it will be used (newsletter), and for what frequency (monthly).

2. Customer Feedback

✗ **Broad Purpose:** "We collect customer feedback to enhance our services."
Issue: While the goal is positive, the lack of precision or specificity about how the feedback will be used, whether it will be analysed individually, and for what specific services or improvements can lead to uncertainty and potential misuse.

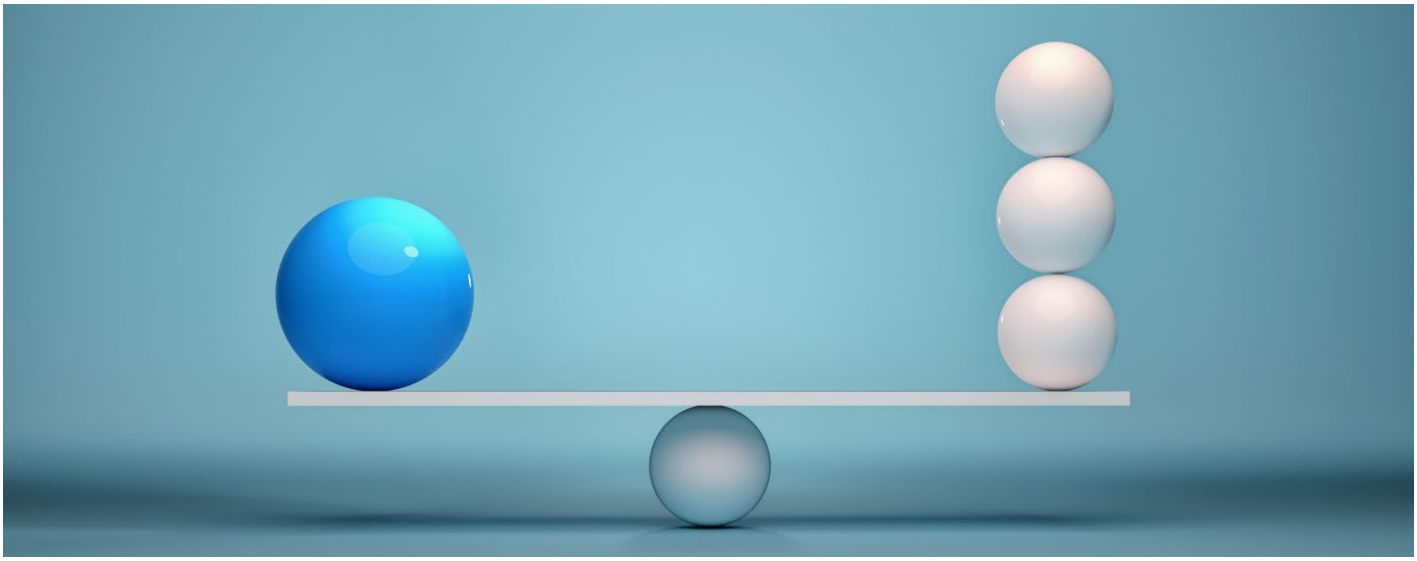
✓ **Specific Purpose:** "We collect customer feedback through surveys to improve our customer service quality by analyzing responses related to your recent support experience.
Advantage: This specifies the type of feedback collected (related to customer service), how it will be used (to improve service quality), and the context (recent support experience).

If the principle of Data Minimisation is adhered to, do we need to evaluate Purpose Limitation?

In our world of today, organisations are encouraged to have clear business objectives to enable them limit the data they collect to what is necessary to achieving their business objective.
When organisations achieve their main objective for processing personal data, they have to be careful not to extend the purpose of processing to other types of processing they did not set out to do from the onset.

Why do we need to evaluate both?

Data minimisation ensures you are not collecting excessive data, while Purpose Limitation ensures that the data collected is used strictly for its intended purpose. Both principles work together to ensure data is handled responsibly.
In general, there are actions that organisations ought to take when processing personal data for a purpose other than what was communicated to the data subject. These actions include establishing a new lawful basis of processing personal data and informing data subjects of the additional processing activities. This would ensure that even when minimal data is collected and used strictly for its intended purpose, the organisation does not violate to the Nigeria Data Protection Act in the event that the organisation wants to use the data for an additional business reason.



Case Study 2

The local government's chapter of a political party starts a petition for improvements in public transportation in a busy urban neighborhood. They deploy a web form to collect personal data such as name, age, address, names of children, income band of next of kin, of individuals living and working within its environs. The individuals are informed via the webform that their personal data collected will be used for the purpose of the petition. Individuals are also encouraged to sign the petition and share within their circles for a wider reach. A few months later, at the next general election, this local chapter shared the personal data of all those who signed its initial petition, with its state's body, in a bid to show their support for the state body's candidate for Governor. The party's state headquarters informs its subordinates across its local government chapters in the state that it has found that people who care about public transportation are more likely to support the party's governorship candidate. The political party uses the names and addresses it obtained from the petition to send these individuals campaigning leaflets.

Key Observations

- The local chapter of the political party appears to have collected personal data such as names of children and income band of next of kin, beyond the required use thereby violating the principle of Data Minimisation which mandates that only necessary data be collected and processed.
- Sending campaign leaflets to individuals that consented to the collection and use of their information for the petition on improvements of public transport in their local area is a clear case that contravenes the principle of Purpose Limitation. The party is therefore not expected to use this data unless they take further steps to comply with the requirements of the NDPA.
- Finally, the fallout of the wrongful usage of personal data collected from individuals could lead to regulatory fines from the NDPC and reputational damage.

How could these be better managed?

- The local chapter of the political party should review the organisation's data collection forms to ensure that the organisation is not over-collecting personal data beyond the original purpose.
- The local chapter of the political party should ensure that data collected is only used for the specific communicated purpose. Additionally, if a new purpose arises that was not originally communicated, the political party should ensure a lawful basis is established before personal data is used for the new purpose.
- The local chapter of the political party will also need to regularly review the data collected to ensure it remains relevant and necessary for the stated purpose.

Some enforcement sanctions on the breach of Data Minimisation and Purpose Limitation principles around the Globe

1. In June 2024, the Spanish Data Protection Authority – AEPD imposed a fine of €2,000 on EXPLOTACIONES HOSTELERAS Y DE OCIO ALBACETEÑAS, S.L. The controller had installed video surveillance cameras which, among other things, also covered the public space. The DPA considered this to be a violation of the principle of Data Minimisation. The DPA also found a breach of the controller's obligation to provide sufficient information on data processing under Art. 13 GDPR. (https://www.enforcementtracker.com/ETid-2417)

2. In May 2019, the Belgian Data Protection Authority (APD/GBA) fined a local political association €3,000 for violating the principle of Purpose Limitation. The association sent election advertisements to residents of a municipality during the 2018 local elections. The association violated the principle of Purpose Limitation by using electoral rolls it obtained from residents in 2012. Residents had previously provided their personal information for electoral purposes in 2012 not for receiving political advertisements. (https://gdprhub.eu/index.php?title=APD%2FGBA_%28Belgium%29_-_39%2F2020)

3. In 2019, the Hungarian National Authority for Data Protection and the Freedom of Information (NAIH) levied a fine of €3,200 against a financial institution for unlawfully rejecting a customer's request to have his phone number erased after arguing that it was in the company's legitimate interest to process this data in order to enforce a debt claim against the customer. In its decision, the NAIH emphasised that the customer's phone number is not necessary for the purpose of debt collection because the creditor can also communicate with the debtor by post. Consequently, keeping the phone number of the debtor was against the principles of Data Minimisation and Purpose Limitation. As per the law, the assessed fine was based on 0.025% of the company's annual net revenue. (https://www.enforcementtracker.com/ETid-37)

Can You Spot the Non-Compliance?

Below, we will explore various scenarios related to Data Minimisation and Purpose Limitation, drawing on examples observed across multiple organisations. These scenarios would delve into the reasons behind classifying them as either a breach of Data Minimisation or a breach of Purpose Limitation requirements of the NDPA.

S/N	Scenario	Violation of Data Minimisation and/or Purpose Limitation?	Why?/Why not?
1	A hospital collects detailed personal information from patients during registration, including medical history, current medications, allergy information, and name of employer. This information is used solely for providing medical care and determining the patient's eligibility for certain treatment plans.	No	The hospital collects only necessary information for medical care and uses it solely for that purpose, adhering to both Data Minimisation and Purpose Limitation requirements.
2	A bank collects customer data to process loan applications, including financial history, credit scores, and name of employer. The data is used solely for evaluating the customer's loan eligibility, and once the loan process is completed, the data is securely deleted or archived for a legally required retention period. The bank does not use the data for any other purpose, such as marketing or sales of the data to third parties.	No	The bank collects only the data necessary for loan processing and uses it exclusively for assessing loan eligibility, ensuring customers are informed about how their data will be used and not sharing it externally without a legitimate reason.
3	An online retail platform requires customers to provide their full birthdates, home addresses, and payment details to create an account. This information is also used for marketing campaigns and shared with third-party advertisers without obtaining explicit consent from the customers.	Yes, both	The platform requires unnecessary personal data to sign up (home addresses) and uses it for purposes (marketing and sharing with third parties) beyond what was initially stated, violating both principles. Additionally, it would be ideal to obtain the customer's delivery address, and this should be obtained at the checkout point rather than at account creation.
4	A healthcare provider collects patients' data for administering healthcare services. This data is used solely for medical treatment purposes only. However, on the hospital registration form, data fields like ethnicity, patient's political party, and religion are being captured.	Data Minimisation only	The healthcare provider does not comply with the principle of Data Minimisation as personal data such as ethnicity, patient's political party, and religion are generally not required to provide medical treatment to a patient.
5	A ride-hailing app that collects a user's real-time location only when a ride is requested, limiting unnecessary tracking has begun to target users with location-based advertisements, such as promotions for nearby restaurants or entertainment venues.	Purpose limitation only	The ride-hailing app does not comply with the principle of Purpose Limitation. It originally collected real-time location data solely to facilitate ride requests but later repurposed it for targeted advertising without relying on a new lawful basis for such processing. By using the data for a different objective—location-based ads—the app processed data beyond the original purpose for which the data was collected.

Key Considerations for organisations to ensure compliance

1. **Maintain a Personal Data Asset Inventory**
   Maintaining a Personal Data Asset Inventory (i.e. Record of Processing Activities) plays a critical role in giving organisations the right level of visibility to question and evaluate their data collection across various processing activities. The inventory helps organisations see the data being collected, the purpose of collection, the medium via which the data is collected, etc., which aids organisations in complying with the Data Minimisation and Purpose Limitation principle. Organisations are encouraged to document the categories of personal data collected, stored, and processed and ensure records are updated regularly for accountability and transparency. A well-maintained Personal Data Asset Inventory enables organisations to identify redundant or excessive data collection by mapping out what data is being collected and assessing whether it is essential and document the intended purpose of each data category to prevent unauthorized repurposing.

2. **Undertake Data Protection Impact Assessment (DPIA)**
   A well-conducted DPIA ensures that personal data is collected, processed, and retained only to the extent necessary for a specific, lawful purpose. Conducting a DPIA helps to identify excessive data collection, eliminate redundant or unnecessary data, optimize data collection practices within an organisation, highlight potential misalignments between stated purposes and actual data usage etc. Organisations are encouraged to undertake DPIAs to evaluate the necessity and proportionality of the data being collected before they undertake processing of such data, as this would significantly help them adhere to the Data Minimisation and Purpose Limitation principle.

We would love to have your take

1. What challenges have you experienced in your attempt to comply with the Purpose Limitation principle and how are you managing those?
2. Are there any key insights that organisations can take in complying with Data Minimisation principle?
3. As a data subject, have you ever experienced a breach of Data Minimisation or Purpose Limitation? Share your experience with us!

We would love to hear from you, Kindly provide feedback at https://forms.office.com/e/aYSDNFSz7f

For further information, contact:

John Anyanwu
Partner, Cyber & Privacy
KPMG in Nigeria
T: +234 803 975 4061
john.anyanwu@ng.kpmg.com

Olaoluwa Agbaje
Senior Manager, Cyber and Privacy KPMG in Nigeria
T: +234 816 960 8200
Olaoluwa.Agbaje@ng.kpmg.com

Contributors

Kudirat Tobi Mustapha
Cyber & Privacy
kudirat.mustapha@ng.kpmg.com

Sandra Eke
Cyber & Privacy
sandra.eke@ng.kpmg.com

Joseph Oforma
Cyber & Privacy
joseph.oforma@ng.kpmg.com

Joshua Emokpare
Cyber & Privacy
joshua.emokpare@ng.kpmg.com

Kolisenye Nwaboku
Cyber & Privacy
kolisenye.nwaboku@ng.kpmg.com

home.kpmg/ng
home.kpmg/socialmedia

Download on the App Store