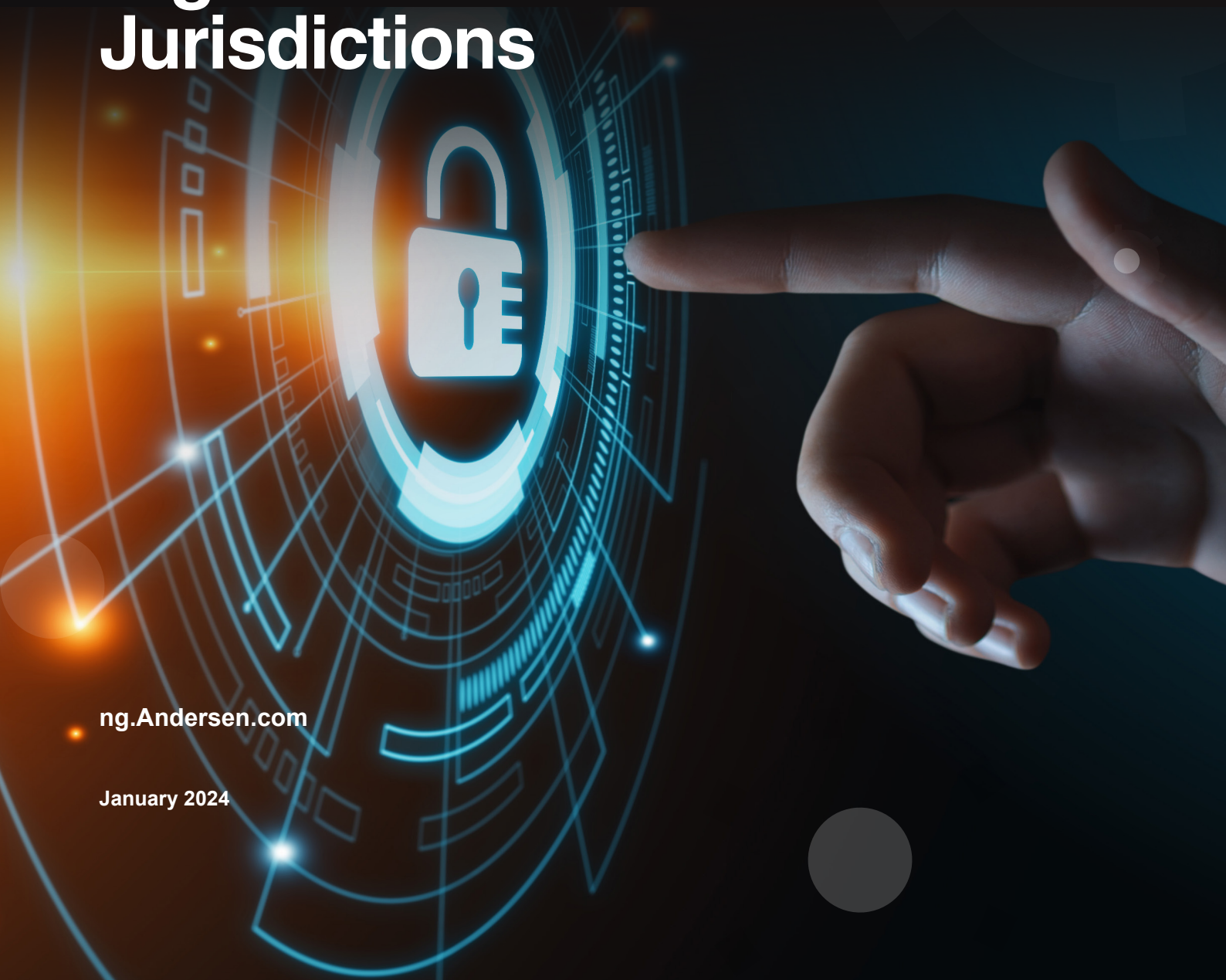
ANDERSEN®

An Overview of the Recent Developments on Data Privacy in Nigeria and other Select Jurisdictions



ng.Andersen.com

January 2024

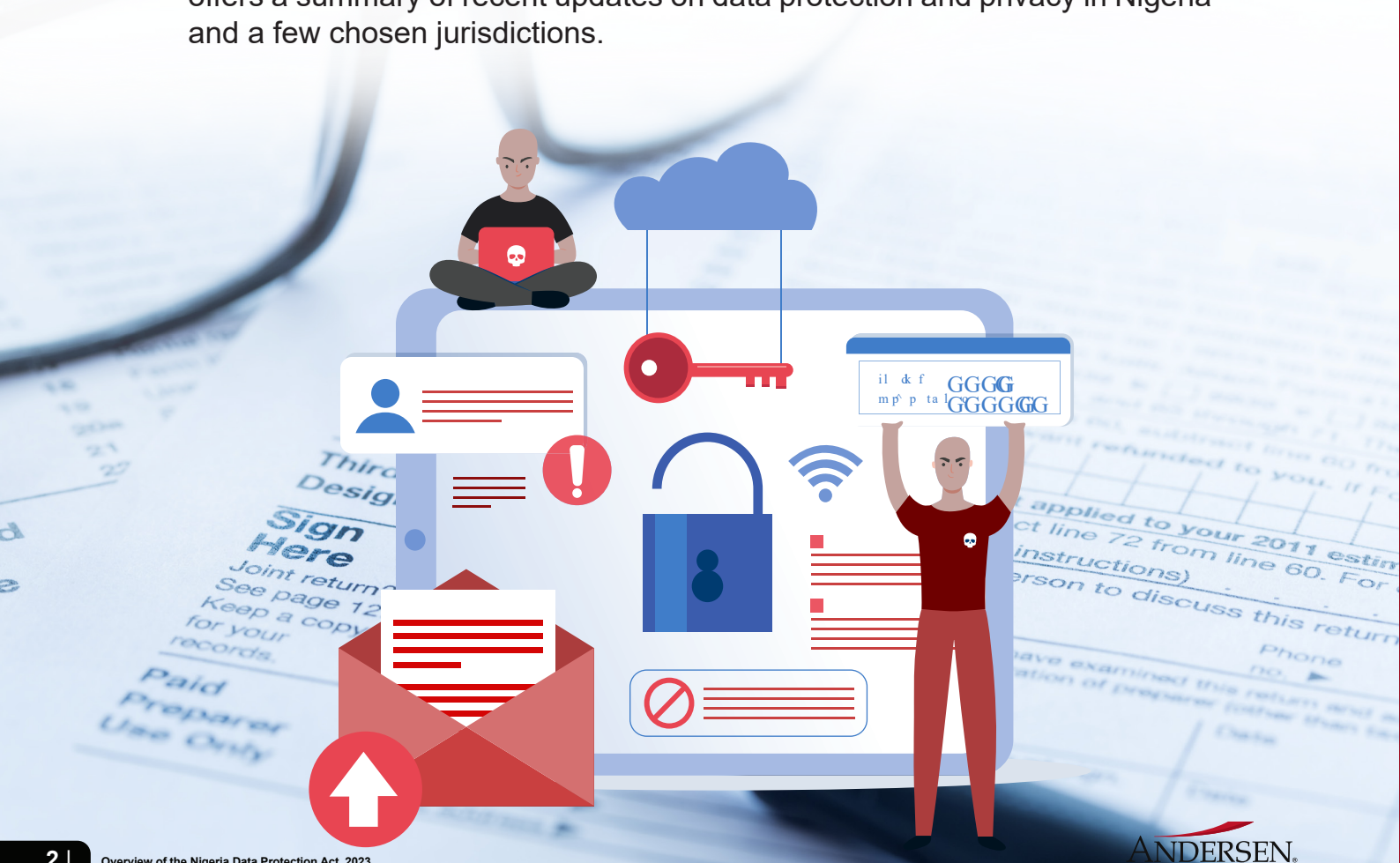
Introduction

In an era where information is the new currency, the evolution of data protection has become a paramount narrative shaping the landscape of our digital world.

Given the rapid technological advancement and the exponential surge in data dependency of companies operating within the financial services, healthcare and technology ecosystems at the global stage, there has been a clarion call from stakeholders such as customers and regulators for data-driven companies to take a more proactive and systematic approach focusing on data governance, cybersecurity and information technology architecture, in ensuring the adequate protection and security of data within their possession.

Furthermore, 2023 witnessed significant development in the data protection space within Africa and Nigeria with the recent ratification and coming into force of the African Union Convention on Cyber Security and Personal Data Protection and the passage into law of the Nigeria Data Protection Act, ("NDPA") in June 2023.

In commemorating the 2024 International Data Privacy Day, this newsletter offers a summary of recent updates on data protection and privacy in Nigeria and a few chosen jurisdictions.



ANDERSEN

Part A

Highlights of Key Data Privacy Updates in Nigeria

1. Enactment of the Nigeria Data Protection Act 2023

On June 12, 2023, President Bola Ahmed Tinubu, GCFR, signed the Nigeria Data Protection Act ("NDPA" or "Act"), 2023 into law. The Act establishes a legal framework for safeguarding personal information and establishes the Nigeria Data Protection Commission ("NDPC" or "Commission") to regulate the processing of personal information.

Notably, Section 64 of the NDPA contains a transitioning framework ensuring that all regulations, licenses, or orders issued by the defunct Nigeria Data Protection Bureau (NDPB) and National Information Technology Development Agency (NITDA) remain in force until they are repealed, replaced, reassembled, or altered. As a result of the foregoing the Nigeria Data Protection Regulation (NDPR), 2019, which was the primary legislation on data protection in Nigeria, remains in effect.

Significant changes introduced by the NDPA that impact data controllers and processors include:

a. Territorial Scope

The NDPA has removed the NDPR references to the data subject's nationality and limited the applicability of the NDPA to:

- controllers and processors domiciled, resident or operating in Nigeria;
- processing operations taking place in Nigeria; or
- where the data subjects are located in Nigeria and the controller and processors are not domiciled, resident, or do not operate in Nigeria.

b. Legal bases for processing

The NDPA introduces a sixth legal basis referred to as "legitimate interest", as one of the legal/lawful bases for the processing of personal data in Nigeria.
The NPDA, just like its counterpart, the European Union General Data Protection Regulation (EU GDPR) and the United Kingdom General Data Protection Regulation (UK GDPR), introduced the "balancing test" which requires "data controller or data processor, or … a third party to whom the data is disclosed" seeking to rely on legitimate interest to ensure that the pursuit of their own legitimate interest does not override the fundamental rights and freedom of the data subject.

In addition, other conditions that must be satisfied for the reliance on legitimate interest as a legal basis for the processing of personal data to be lawful include ensuring that the legitimate interest is not incompatible with other lawful bases and that the data subject has reasonable expectation that the personal data would be processed in the manner envisaged.

c. *Additional Requirement for Data Protection Impact Assessment*

In addition to the requirement to conduct a DPIA, the Act introduces the requirement for data controllers to consult the NDPC, where a DPIA indicates that processing data would pose a high risk to the rights and freedoms of data subjects.

d. *Reporting Data Breaches*

Where a data controller suffers a data breach, there are specific reporting obligations that such data controller must carry out depending on the perceived impact of the personal data breach. Under the NDPR, there is an obligation on data controllers to report all types of personal data breaches to the data protection authority. The NDPA has however moved away from this position.

There has been a paradigm shift from the data reporting requirement under the NDPR as the NDPA now requires data controllers to only report data breaches to the NDPC where such data breaches will result in a risk to the rights and freedoms of the data subjects.

Based on the provisions of Section 40 (3) of the NDPA, where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the data controller is required to immediately communicate the personal data breach to the data subject(s) including advice about measures the data subject(s) could take to mitigate effectively the possible adverse effects of the data breach. Therefore, data controllers are expected to carry out a detailed assessment under the supervision of the Data Protection Officer (DPO) or privacy team, to ascertain the extent of the breach in order to determine the appropriate remedial actions to be taken including reporting the data breach to the NDPC within 72 hours.

e. *Processing of Sensitive Personal Data under the NDPA*

As part of the purposive intention of the legislative draftsmen to further safeguard the processing of sensitive personal data such as health, genetic, biometric data etc, section 30 of the NDPA codifies specific grounds under which data controllers or data processors (including sub-data processors) can process sensitive personal data and these include:

- where the data subject has given and not withdrawn consent for the processing activity;
- where the processing is necessary for reasons of substantial public interest on the basis of a law or where the processing is necessary for public health;
- where the processing is necessary for the performance of the data controller's obligations or the existing rights of the data subject under employment or social security laws or any other similar laws;

- where the processing is carried out by a non-profit organisation with charitable, educational, literary, artistic, philosophical, religious, or trade union purposes in the course of its legitimate activities;

- where the processing is necessary to protect the vital interests of the data subject or another person; and

- where the processing is carried out for purposes of medical care or community welfare and undertaken by or under the responsibility of a professional owing a duty of confidentiality.

f. International Data Transfers

Under the NDPR, NITDA had the overall responsibility in deciding which jurisdictions ensured an adequate level of data protection. In the NDPR implementation Framework, NITDA came up with a "White List" containing countries with adequate data protection laws that data controllers and processors in Nigeria can transfer personal data to.

Whilst the NDPA retains the adequacy requirement, NDPA has introduced other mechanisms for international data transfer such as the adoption of binding corporate rules, contractual clauses, a code of conduct, or a certification mechanism. In addition, the NDPC may impose further restrictions on the international transfer of certain categories of personal data.

Under the NDPA, other bases for transferring personal data outside Nigeria in the absence of adequate protection include:

- obtaining explicit consent from the data subject;

- transferring data for the performance of a contract;

- transferring data for the sole benefit of a data subject where obtaining consent is not reasonably practicable and where reasonably practicable, the data subject would likely give consent;

- transferring data for public interests, for the establishment, exercise, or defence of legal claims; and

- transferring data to protect vital interests of data subjects or other individuals who are physically or legally incapable of giving consent.

2. Overview of the Incorporated Trustees of Ikigai Innovation Institute v. NITDA

In our December 2023 Regulatory Alert, we examined the Federal High Court's decision in the case of Incorporated Trustees of Ikigai Innovation Institute v. National Information Technology Development Agency ("Ikigai's case") where the Court held that NITDA acted outside its own rules as provided in the NDPR by designating some countries without an adequate data protection legislation and supervisory body to be contained on the White List. This led to the Court nullifying the part of the White List containing countries like Guinea-Bissau, Sierra-Leone, Togo, etc.

The NDPC Whitelist is a list that contains the countries deemed to have adequate Data Protection Laws. This includes countries that are signatories to the Malabo convention 2014; all EU and European Economic Area Countries; United States of America; Japan and many more.

The Court's decision has significant implications for organizations involved in cross-border data transfers. It necessitates a careful approach to ensure that personal data is not transferred to countries deemed inadequate in terms of data protection legislation. Therefore, it is imperative for organizations to stay informed about these changes as they impact the processing of personal data. Other acceptable mechanisms for the cross-border transfer of personal data such as binding corporate rules, contractual clauses, code of conduct, or a certification mechanism may be considered by data controllers and data processor.

3. Recent Operational Activities introduced within the Data Protection Space in Nigeria

a. Registration of Data Processors and Data Controllers with the NDPC

On 11 January 2024, NDPC unveiled the pilot NDPC Information Management Portal (Portal) during the stakeholder meeting with representatives of Data Protection Compliance Organizations (DPCOs).

The Portal which is expected to serve as the official platform for the registration of "Data Controllers and Data Processors of Major Importance" in accordance with Section 44 of the NDPA, covers the registration of the Company, its data processing activities, the DPO(s), its safety measures and verification.

The Commission intends to begin the registration process at the end of the current audit cycle i.e. from 15 March, 2024. Therefore, Data Controllers and Data Processors will be required to put in place relevant measures to ensure prompt registration with the NDPC and avoid any regulatory infractions for non-compliance.

b. Certification of Data Protection Officers

During the stakeholders meeting with the DPCOs, the Commission emphasized the need for registration process to be restricted to DPOs who have undergone relevant data privacy and protection certification from internationally recognized data protection certification bodies.

The Commission is however working on standardizing the national data protection certification process/framework in Nigeria, which is expected to be integrated into the Portal.

The Commission is expected to issue a user guideline containing more information relating to the functionality of the Portal in order to aid in the timeous completion of the registration process.

c. Nigeria Data Protection Comission Guidance Notice On The Filing Of Data

On 15 November 2023, NDPC pursuant to the provisions of Section 6 the NDPA released a Guidance Notice (NDPC/HQ/GN/VOL.01/23) in view of the new cycle of Compliance Audit Return ("CAR") filing which will begin this year and serve as a guide to Data Controllers and Processors in the fulfillment of their obligations as stipulated under the NDPA and NDPR respectively.

The main points contained in the Guidance Notice are:

i. A Reiteration on the Reliance of the Provisions of Articles 4.1(5) and (7) of the NDPR in Filing of CAR by Data Controllers and Data Processors

   The Notice emphasizes that NDPR remains the legal bases for the filing of CAR by Data Controllers and Data Processors who processed the personal data of more than 2000 Data Subjects in a period of 12 months

ii. CAR Focus Areas

   The Notice further emphasizes the focus areas for CAR to include: awareness, capacity building, privacy policy, compliance directives to employees; contractors; agents; etc, due diligence to be conducted for agents and contractors being engaged for data processing. Agents or contractors of Data Processors are also required to provide details of their technical and organizational measures in the form provided by NDPC.

iii. Compliance Memorandum

A Data Controller and Data Processor not later than 24th March 2024, may map out a time bound intention to regularize its data processing activities in line with the NDPA.

iv. Default Fee

The Notice whilst restating the statutory deadline for the filing as 15th March of every year imposed a default fee of 50% of the filing fees to be paid by Data Controllers for failing to file on or before the deadline of 15th March.

In view of the above, data controllers and processors are required to file their Compliance Audit Returns on or before the 15th of March every year. It is crucial for data controllers and processors to continue to maintain a data compliant posture in line with the statutory deadline for filing and other requirements under the NDPC which will ensure that the data controllers and processors remains listed as a data compliance organisation on the NDPC's National Data Protection Adequacy Programme (NaDPAP) Whitelist.

4. Issuance of Code of Conduct by NDPC to DPCOs

In December 2023, the Nigeria Data Protection Commission issued a Code of Conduct for DPCOs (Code of Conduct). The Code of Conduct outlines a range of compliance services that DPCOs may provide including raising awareness and building capacity; facilitating the registration of data controllers or processors with the Commission; developing and implementing compliance schedules; conducting compliance audits; performing data privacy impact assessments; and vetting data privacy agreements. The Code of Conduct aims to harmonize and standardize the framework under which DPCOs discharge their functions.

The Code of Conduct also sets down the responsibility of DPCOs to clients relating to the provision of data privacy and protection services. Some of these responsibilities imposed on DPCOs include:

- Carrying out tasks promptly, diligently and in accordance with high professional standards; and

- Bringing all relevant notices or regulatory instruments to the attention of the data controller or processor, amongst other responsibilities.

5. Central Bank of Nigeria's Requirement for Banks to Collect Social Media Handles of Customers as Part of its Customer Due Diligence

In our article published in June 2023, we analysed the legality or otherwise of the Central Bank of Nigeria (Customer Due Diligence) Regulations, 2023. One notable provision in the regulations is the requirement for customers to provide their social media handles as part of the Know Your Customer (KYC) process.

This requirement sparked a lot of controversy and debate. Some concerns raised include the extent of CBN's authority, the constitutionality of the Regulation, and their compatibility with the NDPA and the NDPR. While the goal of the Regulations is to strengthen Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) standards in financial institutions, there has been pushback from stakeholders such as the National Assembly and the NDPC.

Critics argue that the regulations are unnecessary and infringe upon the rights to freedom of expression and privacy guaranteed under Section 37 of the 1999 Constitution of Nigeria as amended. They also claim that the regulations go against the principle of minimal data collection (Data Minimization) outlined in existing data protection laws in Nigeria.

Given the criticisms, it is expected that CBN, being the apex regulator of the banking industry, will review the new CDD requirements and possibly make them optional. Banks and financial institutions should be proactive in jointly engaging with the CBN and the NDPC to determine whether to comply with the Regulation or wait for its withdrawal or specific instructions from the NDPC being the primary regulatory of data protection in Nigeria.

Part B

Asides Nigeria, Data Protection and Privacy Witnessed Significant Developments in other Jurisdictions

Some of the highlights include:

1. The Coming into Effect of the African Union's Malabo Convention on Cyber Security and Personal Data Protection ("Malabo Convention" or "Convention")

The Malabo Convention was adopted by the African Union (AU) Assembly in 2014.

Despite the laudable attempt at further strengthening the data protection legal framework within the African continent, Malabo Convention only recently came into effect, 9 years after its adoption, following Mauritania's ratification being the 15th African country to conclude the ratification of the Convention.

The simple explanation for the delay in the implementation of the Convention can be traced to the provision of Article 36 of the Convention which provides that the Convention shall come into force "30 days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification." The 15th ratification was received from Mauritania on 19th April 2023 and subsequently deposited with the AU on 9th May 2023 and therefore steering the course for the implementation of the Convention across Africa.

The Malabo Convention aims to promote a safe and secure digital environment in Africa. It sets guidelines for data protection, preventing cybercrime and promoting cooperation among African countries. To give credence to this point, the preamble to the Convention emphasizes the need for a harmonized legislation by African member states which will ensure that the data protection legal framework in Africa remains consistent with the African legal, cultural, economic and social environment following the accession to the Convention by African member states.

Although Nigeria is among the list of countries yet to ratify the Convention, the coming into effect of the Malabo Convention is a significant development as it marks the first legal instrument relating to data privacy protection to be enacted at the continent level.

2. Provisional Approval of the First Draft of the European Union Artificial Intelligence Act

The past decade has witnessed an increased use of Artificial Intelligence (AI) by companies and organisations to process data as well as by security and Border Patrol Agencies for the prevention and combating of crimes. The European Union

Artificial Intelligence Act (EU AI Act) was first approved by the European Commission in April 2021 and in December 2023 an agreement was had on the final version of the draft Act.

The Act is the first wholistic regulation that seeks to regulate the use of Artificial Intelligence in the European Union (EU). The priority of the European Commission is to ensure that the AI systems used in the EU are safe, transparent, traceable, non-discriminatory and protect the fundamental human right of EU citizens emphasizing the need for human oversight to prevent any harmful outcomes.

The rule establishes obligations for providers and users depending on the level of risk from artificial intelligence. Transparency requirements to be complied by Generative AI, like ChatGPT, include:

- Disclosing that the content was generated by AI;
- Designing the model to prevent it from generating illegal content; and
- Publishing summaries of copyrighted data used for training.

The EU AI Act is expected to come into force in 2025. It is therefore imperative for data controllers and processors processing personal data of EU citizens under an intragroup processing arrangement through the use of AI for instance, to take proactive steps towards ensuring the seamless integration of the requirement under the EU AI Act once enacted, into their existing data protection processes, policies etc.

3. EU Commission Designates 17 Companies as Very Large Online Platforms under Digital Service Act

The Digital Services Act (DSA) which came into effect on 16 November, 2022, following the approval of the European Parliament and Council, aims at protecting users' rights online and ensuring that online platforms are accountable. It establishes rules for digital services, such as marketplaces, that connect consumers with goods, services, and content. It creates a unified framework across the European Union (EU) and therefore streamlining the provision of digital services.

The European Union Commission set a deadline for 17th February 2023 for all online platforms and online search engines to publish their user numbers in the European Union. This was done to determine whether online platforms and online search engines may be Very Large Online Platforms (VLOPs) or Very Large Online Search Engines (VLOSEs) under the DSA. The DSA classified VLOPs and VLOSEs as those reaching more than 10% of the EU's population or 45 million users.

Some of the Companies classified as VLOPs include:

- AliExpress
- LinkedIn
- Appstore
- Snapchat, etc.

Two Companies classified as VLOSEs are:

- Google search and
- Bing

The compliance obligations of VLOPs and VLOSEs under the DSA which are to be complied within a period of 4 months from February 2023 are:

1. Reporting criminal offences occurring on their platforms;
2. Transparency as regards advertising, recommender systems or content moderation decisions and;

3. Establishing a point of contact for authorities and users.

Additionally, they are required to identify, analyse and assess risks linked to their services particularly risks related to:

a) Illegal content

b) Fundamental rights, children's rights and consumer protection

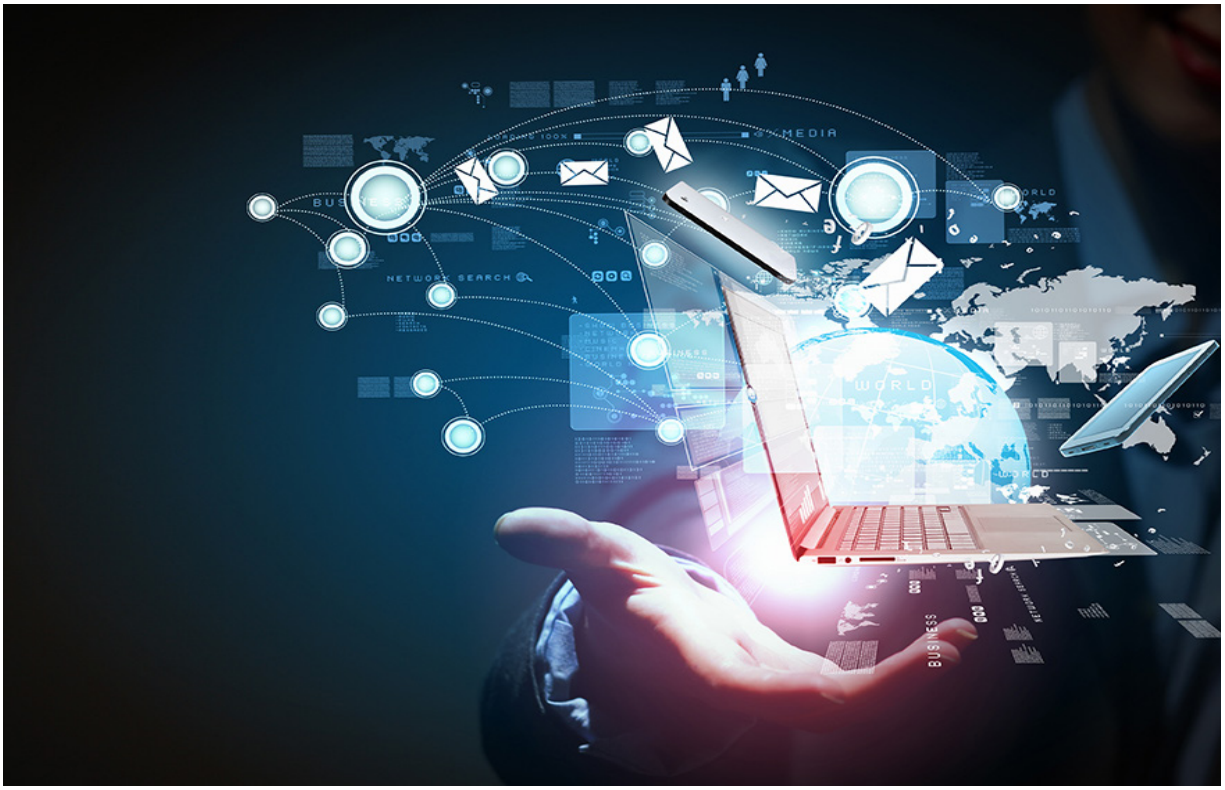
c) Gender based violence, public health protection of minors and mental & physical wellbeing etc amongst other responsibilities.

The DSA will become applicable for all covered services from 17th February 2024.

4. Adoption of the Adequacy Decision for the EU-US Data Privacy Framework by the European Commission

On July 2023, the European Commission adopted its "Adequacy Decision" for the EU-US Data Privacy Framework (DPF). An Adequacy Decision is basically a decision by the European Commission to determine whether a country outside the European Union offers an adequate level of data protection.

The EU-US Data Privacy Framework governs the transfer of personal data between the EU and the US. This Framework is a welcome development as it ensures that EU data subjects benefit from practical safeguards and protection as it relates to the processing of their personal when they have been transferred to non-European Countries.
Organisations in the United States are allowed to voluntarily enter the EU-US DPF



and on doing this, compliance becomes compulsory. However, in order to enter the DPF, an organisation must be subject to the investigatory and enforcement powers of the United States' Federal Trade Commission, the Department of Transport or other statutory body that will ensure statutory compliance, amongst other requirements.

5. Enforcement and Imposition of Fines on Major Tech Giants

The second quarter of 2023 came with the imposition of heavy fines and sanctions on major tech companies due to the violation of children's privacy laws. The companies affected by these fines include:

a. Microsoft

In June 2023, a case instituted by the United States Justice Department on behalf of the Federal Trade Commission was resolved against Microsoft Corporation for retaining personal information from children who use Microsoft's Xbox Live service. This led to the issuance of $20 million in civil penalties.

According to a complaint filed in the U.S. District Court for the Western District of Washington, the United States claims that Microsoft was aware that some users were children and Microsoft allegedly collected personal information, like phone numbers, without properly notifying parents or obtaining parental consent. The complaint also suggests that the notice provided to parents was incomplete and did not meet the requirements of the Children's Online Privacy Protection Act Rule (COPPA Rule). Lastly, it is alleged that Microsoft retained personal information of children who started but didn't complete creating Xbox Live accounts for longer than allowed by the COPPA Rule .

The COPPA sets specific requirements for websites or online services that are meant for kids under 13. It also applies to websites or services that know they are collecting personal information from children under 13. The goal of COPPA is to protect the privacy and safety of young internet users.

Therefore, Microsoft will be required to put in place appropriate measures to enhance privacy safeguards for kids using their Xbox system. One of the changes is that COPPA protections will now apply to third-party gaming publishers who receive children's data from Microsoft. The Order of the Court also clarifies that data like avatars created from a child's image, as well as biometric and health information, fall under the purview of the COPPA Rule when collected alongside other personal data.

b. Fine Imposed on TikTok by the Irish Data Protection Commission

In September 2023, an inquiry opened by the Irish Data Protection Commission (DPC) into Tik Tok Technology Limited led to the imposition of €345 million on the tech giant. The imposition of the fine was as a result of failure of Tik Tok to be

transparent with children about their privacy settings. The DPC raised concerns about how TikTok was handling the data of kids. The inquiry specifically looked into TikTok's compliance between July 31, 2020, and December 31, 2020. The DPC enforcement action is aimed at ensuring that TikTok strictly adheres to the rules under the GDPR relating to the processing of personal data of child users particularly in the context of:

- Certain TikTok platform settings, including its default public settings applied to child users' accounts; and

- Incorporating age verification as part of the registration process

6. Reprimands Issued by the United Kingdom's Information Commissioners Office for Data Breaches

The Information Commissioners Office has enforcement powers as contained in the Data Protection Act of 2018 to conduct investigations, issue warnings, reprimands, notices and fines. Recently, several organisations have been investigated and reprimanded by the Commission for data breaches. Some of the reprimands issued include:

a. Charnwood Borough Council

In November 2023, the United Kingdom's Information Commissioners Office (the Commission) issued a reprimand to the Charnwood Borough Council (the Council) for the disclosure of the new data subject's address to an ex-partner who the data subject has previously accused of domestic abuse. The breach occurred when the Council erroneously sent a correspondence to an old address the data subject shared with her previous partner. The data subject has previously informed the Council of the allegations of domestic abuse and the move to a new address. In the reprimand issued by the Commission, the Commission recommended to the Council to train all staff who deal with vulnerable service users on the handling of personal data, amongst other remedial actions.

b. National Health Service Fife, Scotland

The Commission also issued a reprimand to the National Health Service (NHS) in Fife, Scotland after an unauthorized individual gained access to a ward and accessed the information of 14 patients. The reprimand issued by the Commission includes for NHS to review and update its policies regarding Identity card verification for staff, data breach reporting process amongst other recommendations.

Our Thoughts

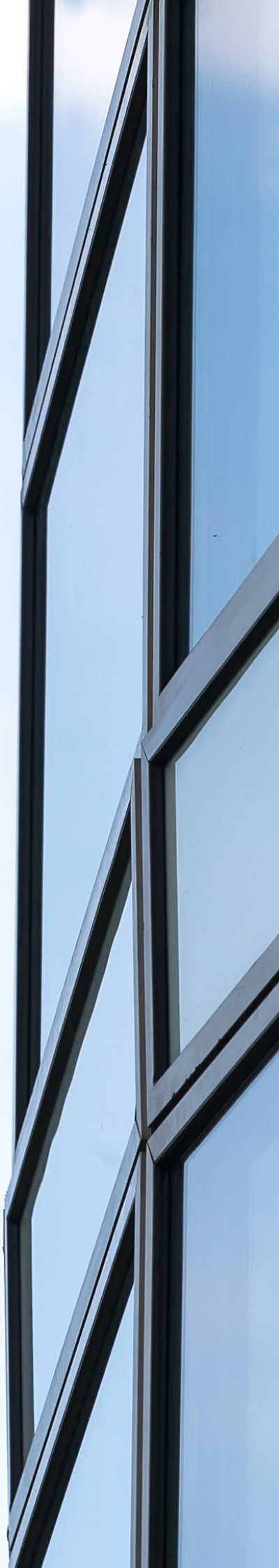
Given the heightened activities of the NDPC and the issuance of regulatory sanctions for data privacy infringements globally and locally in 2023, we anticipate a surge in data privacy initiatives.

In light of this, it is crucial for Data Protection Officers (DPOs) in both local and multinational companies to maintain their organizations' compliance as data controllers with the NDPA and other relevant data protection regulations. Embracing global best practices in organizational and technical measures for data processing activities in Nigeria becomes paramount. By doing so, associated risks of non-compliance with the NDPA, such as reputational damage, regulatory fines, or legal action resulting from data breaches, can be effectively mitigated or eliminated

Conclusion

In a nutshell, the continuous developments in the data privacy scene, both in Nigeria and across jurisdictions, highlight the growing importance of protecting individuals' personal data in the digital age. These updates in the data privacy space reflect a global trend towards stricter regulations and enforcement actions against big tech companies.

Enhancing current data protection and privacy processes, policies, and systems remains crucial for companies. It is imperative that they conduct thorough data protection and privacy audits, submitting their audit reports by the regulatory deadline of March 15, 2024. This ensures alignment with the stringent stipulations of the NDPR, mitigating the potential risks of regulatory sanctions which may result to the imposition of fines as well as averting reputational harm and business disruptions.



For comments and questions, please contact:

Michael Ango
Partner
Tax Advisory & Regulatory Services
E: michael.ango@ng.andersen.com

Samuel Ibrahim
Senior Manager
Tax Advisory & Regulatory Services
E: Samuel.Ibrahim@ng.Andersen.com

Emmanuel Omoju
Senior Manager
Tax Advisory & Regulatory Services
E: Emmanuel.Omoju@ng.Andersen.com

Patience Aliu
Manager
Tax Advisory & Regulatory Services
E: Patience.Aliu@ng.Andersen.com

Lagos, Nigeria

47 Glover Road, Ikoyi.
t: 0913 800 7000
(+234) 700TAXADVISERS

Abuja, Nigeria

Yobe Investment House, Suite 302,
Plot 1332 Ralph Shodeinde Street,
Central Business District, Abuja.

info@ng.andersen.com
marketing@ng.andersen.com

ng.Andersen.com

ng.Andersen.com/socialmedia