ANDERSEN®

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

January 2023

ng.andersen.com

All over the world, technological advancements and breakthroughs have increased exponentially, which has increased the use of personal data and associated risk of data breaches. Thus, data protection and privacy continues to gain global attention due to the compliance obligations and responsibilities that come with data processing activities.

As a result, we have witnessed increased efforts by various governments to ensure compliance with data protection laws across different jurisdictions and significant strides being recorded by corporations to formulate and implement robust data protection compliance framework for the processing of personal data within their possession.

Protecting the privacy of personal data is the responsibility of every business. Therefore, all data controllers are expected to take appropriate actions towards creating a culture of privacy within their environment. As we celebrate the 2023 International Data Privacy Day, this Newsletter provides highlights of recent data protection and privacy update in Nigeria and across few select jurisdictions.

Part A - Highlights of Key Data Privacy Updates in Nigeria

1. *Overview of the ECOWAS Law Suit Seeking to Compel the Federal Government of Nigeria to Enact a National Legislation on Data Protection*

On the 19 July 2021, a registered Non-Governmental Organisation (NGO), Incorporated Trustees of Digital Rights Lawyers Initiative (the "DRLI"), instituted a public interest lawsuit at the ECOWAS Court in Suit No: ECW/CCJ/APP/37/21 and sought an order of Court compelling the Federal Government of Nigeria to enact into law a

comprehensive data protection legislation in order to protect and enforce the data privacy rights of Nigerians.

The DRLI in its arguments referenced the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS ("Supplementary Act") which Nigeria signed along with another West African Countries on 16 February 2010. The Supplementary Act, which is believed to be the first regional instrument promoting the protection of the data privacy rights of citizens of ECOWAS Member State, requires each Member States to establish a legal framework for the protection of data privacy rights within the ECOWAS.

DRLI alleged that the Nigerian government had failed to fulfil its obligation as a Member State to enact a comprehensive national legislation domesticating the provisions of the ECOWAS Supplementary Act.

However, the Nigerian Government, in its counter-argument, denied the allegations of the DRLI and enumerated the extant laws in force for the protection of data privacy in Nigeria. It was also contended on behalf of the Federal Government of Nigeria that the ratification of the Supplementary Act will require legislative approval in line with the constitutional procedure stipulated under Section 12 of the 1999 Constitution of the Federal Republic of Nigeria.

The three-man panel of the ECOWAS Court have reserved Judgment in the suit till 15 March 2023. Whilst it is not in doubt that considerable efforts have made towards the enactment of the Nigeria Data Protection Bill 2022 which is currently undergoing deliberations at the National Assembly, the public interest lawsuit instituted at the ECOWAS Court by the DRLI clearly demonstrates increased level of awareness regarding the importance of data privacy rights within Nigeria and West Africa at large and the resolve of NGOs to challenge the status quo regarding perceived unwillingness of the government of the day to enact data protection laws by way of legal redress both at national and regional courts of law.

2. *Introduction of the Data Protection Bill 2022*

On 6 October 2022, the Nigeria Data Protection Bureau officially released the new draft of the Nigeria Data Protection Bill 2022 ("the Bill"). The Bill provides the legal framework for the processing and protection of personal data in Nigeria.

In terms of the scope of its applicability, the Bill will only apply where:

- the processing of personal data is carried out by a data controller or data processor domiciled, ordinarily resident or ordinarily operating in Nigeria;
- the processing of personal data occurs within Nigeria; or
- the processing of the personal data of the data subject occurs in Nigeria without the data controller or the data processor being domiciled, ordinarily resident or ordinarily operating in Nigeria.

The Bill does not however apply to the processing of personal data for personal or household purposes as well as in cases of criminal investigation and prosecution, national public health emergency, national security, public interest or the establishment or defense of legal claims.

The Bill provides for the establishment of the Nigeria Data Protection Commission ("the Commission") to be headed by the National Commissioner, with the Governing Council assuming a supervisory role over the Commission. The Commission is expected to be independent in the discharge of its responsibilities. The Bill also covers key areas such as data protection principles, lawful bases for the processing of personal data, requirements for the processing of sensitive personal data and conducting of a data protection impact assessment, rights of data subjects, appointment of Data Protection Officers ("DPOs") and licensing of data protection compliance organisations ("DPCOs"), rules relating to cross-border transfer of personal data, amongst others.

The Bill confers enormous enforcement powers to the Commission including the powers to arrest, search and seize during the course of investigation.

Due to the national importance of the Bill, it is expected that the National Assembly will expedite the constitutional process for the review of the Bill to enable the Bill receive Presidential assent in due course.

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

a. Establishment of the Nigeria Data Protection Bureau

The Nigerian data protection space witnessed significant regulatory reforms in 2022 with the establishment of a new data protection regulator in Nigeria.

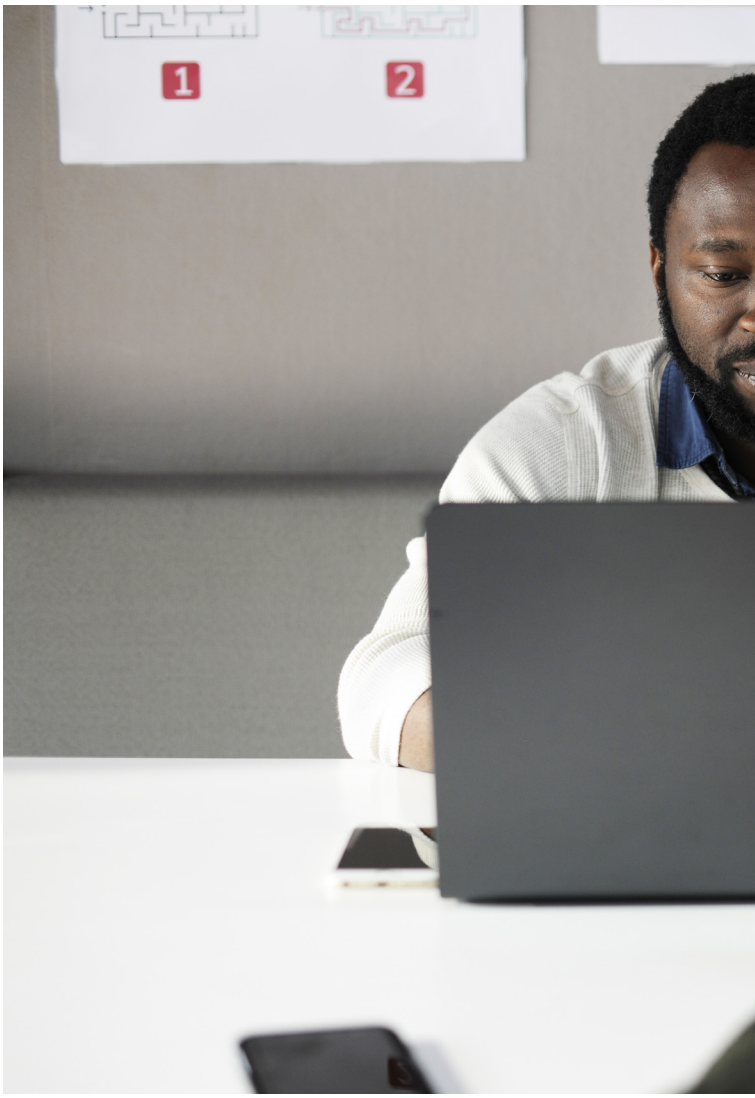
In its official press release made in February 2022, the Federal Government, through the office of the Presidency, approved the establishment of the Nigeria Data Protection Bureau ("the Bureau" or NDPB) following the formal application made by the Minister of Communications and Digital Economy, Professor Isa Pantami. The NDPB was, however, launched in April 2022. According to the official press release, the Bureau will be responsible for consolidating on the gains of the Nigeria Data Protection Regulation 2019 (NDPR) and supporting the process for the development of a primary legislation for data protection and privacy.

Prior to the establishment of the NDPB, The National Information Technology Development Agency (NITDA) was saddled with the responsibility of ensuring data protection and privacy compliance in Nigeria. However, it is noteworthy that the legitimacy of NDPB as the new national data protection regulator in Nigeria has been greeted with criticism as some stakeholders hold the view that the establishment of the NDPB, without any form of statutory backing by way of an enabling law, renders the establishment of the NDPB ineffective ab initio.

Notwithstanding the doubts expressed as to its legitimacy, the NDPB has since assumed the regulatory role of ensuring the compliance with the provisions NDPR and will receive the data protection audit reports from data controllers and processors in Nigeria due on or before the 15 March 2023.

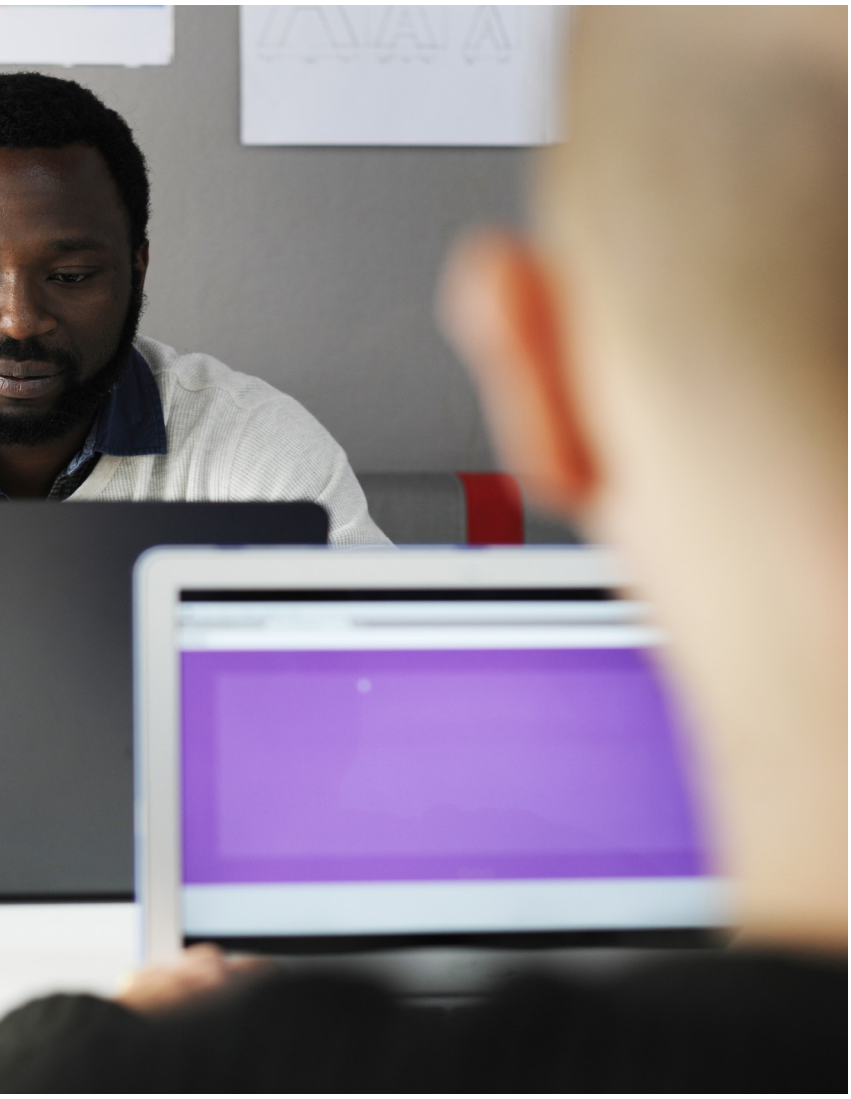
b. Introduction of Electronic Certificate of Compliance by the NDPB

In order to recognise and reward organisations that prioritise conduct of their audits and filing of the audit report,



the NDPB has initiated the process of issuance of electronic certificates to organisations that have complied with their filing requirements in line with the NDPR. Thus, data controllers that conduct their 2023 data protection audit and file the audit report on or before 15 March 2023 with the NDPB will be entitled to receive the electronic certificate. The electronic certificate may be displayed by organisations in their offices and online platforms as a testament of their compliance with the requirements of the NDPR.

The introduction of electronic certificates of compliance by NDPB is laudable and a step in the right direction as it will incentivize organisations to continue to ensure that their data protection and privacy policies, processes and systems are in full compliance with the requirements of the NDPR.



> In order to recognise and reward organisations that prioritise conduct of their audits and filing of the audit report, the NDPB has initiated the process of issuance of electronic certificates to organisations that have complied with their filing requirements in line with the NDPR.

c. The NDPB's Compliance Notice to Data Controllers and Processors

The NDPB, in furtherance of its mandate as the successor agency to NITDA on all matters relating to data privacy and protection in Nigeria, issued a Compliance Notice ("Notice") in November 2022 introducing the National Data Protection Adequacy Programme (NaDPAP or "the Programme"). The Notice was issued pursuant to the NDPR and Section 37 of the Constitution of the Federal Republic of Nigeria, 1999, which guarantees every citizen of Nigeria a Right to Privacy. The Programme represents one of the concerted efforts by the NDPB to create more awareness on the obligations of Data Controllers/ Processors under the NDPR.

Under this programme, the NDPB is expected to compile a Whitelist of organisations in Nigeria that have complied with the requirements of the NDPR which will be published on the NDPB website, in major newspapers, and will be shared with local and international establishments to serve as a reference in relevant transactions and proceedings.

In order to avoid exposure to legal liabilities, the Notice requires organisations to take the following steps:

- Read and understand the NDPR – as it applies to various situations and persons involved in data processing;
- Develop and implement a Privacy Policy that is consistent with the NDPR;
- Notify employees, customers and online visitors of the organisation's Privacy Policy;

- Designate at least one or two members of staff as Data Protection Contacts (DPC), who may, after training, become DPOs of their organisations;

- Forward the names of the DPCs (not more than three) to the Bureau for a free Induction Course in Data Protection Regulation Compliance for Nigeria and the Economic Community of West African States (ECOWAS);

- Mandate service providers (agents, licensees, contractors etc.) to comply with the NDPR;

- Notify the NDPB of the technical and organisational measures it is taking for data privacy and protection).

Furthermore, the Compliance Notice provided a deadline for compliance as organisations that failed to take the steps outlined above and failed to duly notify the NDPB of the technical and organisational measures that they are taking for data privacy and protection on or before 25 November 2022 will not be listed on the NaDPAP Whitelist.

In accordance with one of our core values in providing Best-in-class services, Andersen, as a licensed DPCO, provided support and guidance to its data protection clients in terms of sending out notifications and guidance notes on ensuring compliance with the directives contained in the NDPB's Notice.

4. *Federal Government's Directive to Ministries, Departments and Agencies to Comply with the Nigeria Data Protection Regulation*

In furtherance of its determination to promote the implementation of data privacy and protection practices across Public Institutions in Nigeria, the Federal Government, on 7 November 2022, issued a Circular signed by the Secretary to the Government of the Federation, directing all Ministries, Departments and Agencies ("MDAs") to comply with the provisions of the NDPR.

Notably, the Circular requires all MDAs to ensure that they:

- designate appropriate officers as their DPOs who will on regular basis advise management on data processing activities of their organisation and ensure compliance with the provisions of the NDPR and all matters relating to protection of the privacy, rights and freedom of data subjects;

- forward the name and contact details of the DPOs to NDPB for documentation and requisite induction training;

- appoint licensed DPCOs who will guide the MDA through compliance framework and file their annual reports with the NDPB;

- make appropriate budgetary provision for annual Data Protection Audit compliance process and capacity building of DPOs as well as other staff.

The Circular reinforces the Federal Government's firm commitment towards actualizing the full implementation of the provisions of the NDPR within Public Institutions and it is therefore expected that MDAs, in compliance with Federal Government's directive as contained in the Circular, will commence the process of appointing their respective DPOs and DPCOs in readiness for the 2023 data protection audit and regulatory filing with the NDPB. More importantly, it is expected that this Circular will assist in enshrining a culture of privacy in all public institutions and amongst public servants in Nigeria.

5. ***Data Protection Compliance Requirement for Digital Lending Companies Introduced by the Federal Competition and Consumer Protection Commission***

In accordance with its regulatory powers pursuant to Sections 17, 18 and 163 of the Federal Competition and Consumer Protection Act, 2018 ("the Act") and its bid to clampdown on the illegal loan recovery activities of digital lending companies in Nigeria ranging from customer harassment, encroachment of data privacy rights and criminal defamation, the Federal Competition and Consumer Protection Commission (FCCPC) issued the Limited Interim Regulatory/ Registration Framework and Guidelines for Digital Lending, 2022 ("Interim Digital Lending Guidelines").

Under the Interim Digital Lending Guidelines, companies engaged in digital lending, as part of their regulatory compliance requirement, are mandated to download and complete the prescribed forms with the relevant supporting documents including certificate true copy of the certificate of incorporation, evidence of tax remittance etc.

Importantly, digital lending companies are further required to submit evidence of their data protection audit report filed with the NDPB. The implication of this regulatory compliance requirement is that all new and existing digital lending companies are required to ensure strict compliance with the requirements of the NDPR and lodge their data protection audit report with the NDPB on or before the 15 March due date.

With the issuance of the Interim Digital Lending Guidelines by the FCCPC, it is envisaged that the digital lending space in Nigeria will begin to experience normalcy and adherence to consumer and data privacy rights of financial services end-users.

Part B - Data Protection and Privacy Developments in Other Jurisdictions of the World

1. ***Recent Rulings and Judgments on Data Protection and Privacy***

Away from Nigeria, the global data protection and privacy space witnessed significant activities in 2022, including judicial activism through the pronouncement on key areas pertaining to the rights of data subjects and data retention.

We have highlighted some of the notable rulings emanating from the European Union ("EU") in 2022 below:

- **RW v Österreichische Post AG[1]:** In this case, the Court of Justice of the

[1] Judgment of the CJEU in Case C-154/21 delivered on 9 June 2022

European Union ("CJEU"), in its Ruling, upheld the rights of access of data subjects to obtain from the controller information about the recipients or categories of recipient to whom their personal data have been or will be disclosed.

In this case, RW had requested Österreichische Post, the principal operator of postal and logistical services in Austria, to disclose to him the identity of the recipients to whom it had disclosed his personal data in exercise of his right of access as a data subject under Article 15(1)(c) of the General Data Protection Regulation, 2018 (GDPR).

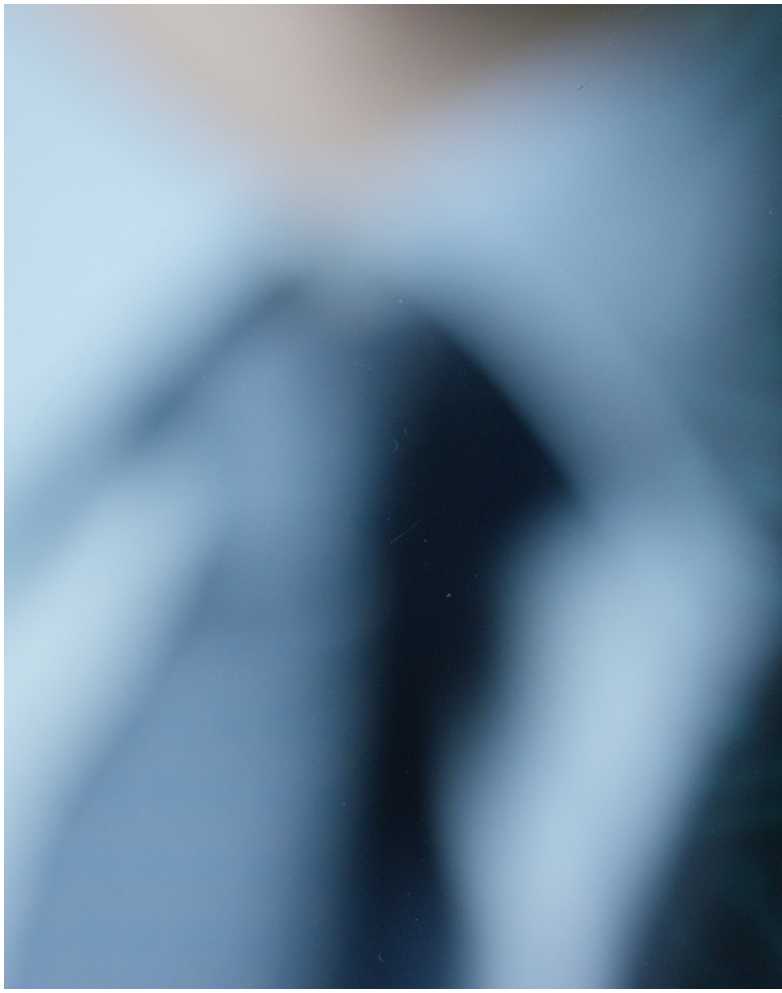
In response to RW's request, Österreichische Post stated that it merely discloses personal data of customers to its trading partners for marketing purposes.

RW brought proceedings against Österreichische Post before the Austrian courts. During the judicial proceedings, Österreichische Post further informed the citizen that his data had been forwarded to customers, including advertisers trading via mail order and stationary outlets, IT companies, mailing list providers and associations such as charitable organisations, NGOs or political parties.

The CJEU, upon receipt of the request for a preliminary ruling by the Supreme Court, Austria, in its Ruling, held that a data controller has an obligation to provide the data subject, on request, with the actual identity of recipients to whom the personal data have been disclosed except where it is impossible to identify those recipients in which case the data controller may indicate only the categories of recipient in question or the request is manifestly unfounded or excessive.

- **Proximus NV v. Gegevensbeschermingsautoriteit (Proximus)**[2] - On 27 October 2022, the CJEU answered questions concerning the interplay between the e-Privacy Directive and the GDPR.

  It held that data controllers should take reasonable steps to inform internet search engines of a data subject's data erasure request. Apart from these steps controllers must implement Technical and Organisation



Measures (TOMs) to inform other controllers who received the data of the withdrawal of consent by a data subject. In instances where multiple controllers rely on the single consent of the data subject, it must be sufficient for the data subject to approach one of the controller to withdraw its consent.

2. Enforcement and Imposition of Fines

The global data protection and privacy landscape, particularly in the EU, experienced significant enforcement actions against defaulting companies for breach of the GDPR and national/sector-specific laws and regulations in 2022. This current state of affairs resulted in the imposition of stiff administrative penalties against such erring companies by data protection regulators.

We have highlighted some of the notable cases involving the imposition of fines by data protection regulators against data controllers ranging from unlawful processing of personal data, failure to communicate personal data

[2] Judgment of the CJEU in Proximus (C-129/21) delivered on 27 October 2022

> **In accordance with one of our core values in providing Best-in-class services, Andersen, as a licensed DPCO, provided support and guidance to its data protection clients in terms of sending out notifications and guidance notes on ensuring compliance with the directives contained in the NDPB's Notice.**

breach to the supervising authority and data subject, accuracy of personal data amongst others.

- *Failure to Notify Data Breach Incident to the Regulator and the Data Subject:* On 3 November 2022 the Polish Supervisory Authority ("PSA") imposed an administrative fine of PLN 250,000 against a telecommunication operator, on P4 SP Z O O, for its failure to notify the PSA and the data subject of the personal data breach.

- *Failure to Respond to Requests from Data Subjects:* On 30 November 2022, the French Data Protection Authority ("CNIL"), after receiving several complaints against a French phone operator FREE regarding its failure to manage customers' requests for access to and deletion of their personal data, imposed a fine of €300,000 on FREE, for several violations of the provisions of the GDPR including contravention of the rights to access, erasure and security of personal data of data subjects.
  Based on its findings, the CNIL also ordered FREE to comply with the GDPR's rules regarding the management of access and erasure requests and to justify this compliance within three months from the decision, with an additional fine of €500 for each day overdue.

- *Accuracy of Personal Data & Transparency Requirements:* On 9 December, 2022 the Finnish Supervisory Authority ("FSA") imposed a fine of €230,000 Euros against a passenger traffic company, Viking Line, for the unlawful processing of employees' health data in breach of the Finnish Data Protection Act.

  The FSA had commenced investigation into the activities of Viking Line based on the complaint received from a former employee of Viking Line alleging that the health data of employees consisting of their diagnosis used in processing information relating to "absence from work due to illness", were uploaded on the HR system for 20 years and that the diagnosis information stored were inaccurate.
  Based on its findings, the FSA ruled that the health data of employees should

have been erased immediately when its storage was no longer necessary noting that inaccurate diagnosis information could pose a risk to an individual's legal protection.

The FSA also discovered that Viking Line had not informed its employees appropriately of the processing of their personal data. The FSA, in addition to the monetary fine, ordered the Viking Line to correct its practices and inform its employees of the processing of their personal data as required under the GDPR.

- *Conducting Advertisement without Obtaining Data Subject's Consent:* *On 29 December 2022*, the CNIL also imposed a fine of €3 Million on a video game publishing company, VOODOO, for using a technical identifier embedded in its mobile applications for advertising without the users' consent in breach of Article 82 of the French Data Protection Act and a fine of €8Million Euros against APPLE DISTRIBUTION INTERNATIONAL resulting from its failure to collect the consent of iPhone's French users (iOS 14.6 version) before depositing and/ or writing identifiers used for advertising purposes on their terminals.

3. *Emerging Artificial Intelligence Technologies and related Privacy Issues*

The emergence of Artificial Intelligence ("AI") as a disruptive technology affords numerous benefits and technical application across several facet of human life such as healthcare, finance, education, social media, entertainment, gaming amongst others. Notwithstanding the foregoing, AI continues to attract strong criticism ranging from cybersecurity vulnerabilities, data privacy, bias and discrimination etc.
One of such AI that has recently gained significant global attention is the OpenAI's prototype chatbot, ChatGPT, launched in November 2022.

ChatGPT is a large language model with the ability to interact in conversational dialogue form and provide responses that can appear human.

The increasing use of ChatGPT for complex activities such as literature writing, coding, etc. has raised immediate concerns ranging from potential copyright infringement arising from plagiarism, generation of discriminatory and offensive content, cybersecurity threat and data privacy and protection concerns.

Some of the immediate data privacy and protection issues that have been identified in the use of chatbot such as ChatGPT include:

- The extent to which the processing of personal data of third-party data subjects on ChatGPT will adhere to the principles of data protection such as purpose limitation, data minimisation, storage limitation, data accuracy.

- The legal basis for the processing of personal data of third-party data subjects hosted on ChatGPT's database, without their prior consent.

- The level of organisational and technical measures implemented in the final version of the ChatGPT (such as encryption, data anoymisation and pseudonymisation) with respect to adequate protection of the personal data of third-party data subjects hosted on its database.

Beyond the regulatory concerns highlighted above, it is expected that Nigeria will witness the increased deployment of AI technology such as ChatGPT within the healthcare, financial, educational, e-commerce sectors. In this regard, organisations intending to leverage on such AI technology for operational efficiency will be required under the NDPR to conduct a Data Protection Impact Assessment ("DPIA") to evaluate the potential risks such technology will pose to the rights and freedom of data subjects.

Our Thoughts

Following the establishment of the NDPB as the "new data protection sheriff in Nigeria" and the increased number of regulatory sanctions involving cases of data privacy rights infringement globally, we expect that the Bureau will continue to build on its predecessor's legacy in 2023 in terms of creating awareness campaigns and sensitizing data controllers/processors on the importance of imbibing data privacy and protection culture within their organisation and clamping down on erring data controllers/processor such as digital lending companies engaged in the unauthorized processing of person data of data subjects as part of their loan recovery process.

Against this backdrop, it is imperative for DPOs of both local and multinational companies to continue to ensure their organisation's adherence, as data controllers, to the NDPR and applicable data protection regulations and adopt global best practice in terms of organisational and technical measures with respect to their data processing activities in Nigeria. In this regard, associated risks of non-compliance with the NDPR such as reputational risk, imposition of stiff regulatory fines or lawsuits resulting from incidence of data breach, amongst others will be mitigated or eliminated.

Furthermore, the synergy between the activities of the Federal Government, through the NDPB and data controllers towards promoting data privacy and protection within the public and private sectors of the economy will invariably position Nigeria as an emerging data privacy and protectionist country on a global scale.

On the whole, the increase in technological advancements through big data and AI technology such as ChatGPT continues to raise numerous data privacy concerns, including issues related to processing of personal data through these emerging technologies. It is therefore not in doubt that 2023 will witness increased regulatory scrutiny and legislative intervention to address the growing data privacy concerns occasioned with the use of AI technologies.

Conclusion

Whilst it is not in doubt that the data protection and privacy landscape continues to gain prominence in Nigeria due to ongoing efforts of the NDPB towards ensuring that companies remain fully compliant with the provisions of the NDPR and the concerted efforts of the Federal Government to enact a national data protection law, it is important for companies to continue to improve on their existing data protection and privacy processes, policies and systems and ensure that they conduct their data protection and privacy audit and file their audit reports on or before the regulatory deadline of 15 March 2023. This is to ensure that the processing activities within their business operations adhere to the strict requirements of the NDPR and to avoid exposure to the risk of regulatory sanctions of up to 2% of gross annual revenue, reputational damage and business disruption amongst other possible negative outcomes which stifle the growth of the company.

For further information, please contact;

Michael Ango
Partner and Head
Tax Advisory & Regulatory Services
E: michael.ango@ng.andersen.com
M: (+234) 803 535 3103

Samuel Ibrahim, PhD
Senior Manager
Tax Advisory & Regulatory Services
E: samuel.ibrahim@ng.Andersen.com
M: (+234) 8164 348 117

Emmanuel Omoju
Senior Manager
Tax Advisory & Regulatory Services
E: emmanuel.omoju@ng.andersen.com
M: (+234) 806 0307 901

Patience Aliu
Manager
Tax Advisory & Regulatory Services
E: patience.aliu@ng.andersen.com
M: (+234) 812 6701 190

ng.Andersen.com

Connect with us

Setting the trend. Shaping the future.

© 2023 Andersen Tax LLC and Andersen Tax LP. All Rights Reserved. Andersen Tax LP, is a Nigerian member firm of Andersen Global, a Swiss verein comprised of legally separate, independent member firms located throughout the world providing services under their own name or the brand “Andersen Tax” or “Andersen Tax & Legal.”