# THE EXPANDING SIGNIFICANCE OF DATA IN THE EMERGING WORLD: ASSESSING THE ROLE OF THE PRINCIPAL ACTORS IN THE DATA PROTECTION ECOSYSTEM.

**Saheed Olamilekan Apampa, Lagos State University**

## ABSTRACT

*The proliferation of data exchange on public and private paper, web and mobile applications, Google, LinkedIn, and Play Store to every social media application whose subscribers are routinely required to provide data to facilitate access portrays the importance and increasing prevalence of data in the modern world. Families, businesses, and governments all need to learn how to live the complexities of a world made possible by cutting-edge technologies and innovative commercial strategies. With real-time intelligence at their disposal, data has been of great value for the characterization, calibration, verification, validation and assessment of creative business models and emerging government policies for predicting their long-term structural durability and performance in extreme situations and a disruptive market environment. To keep up with these expansions of the role of data in all facets of business and non-business functions, provide stronger protection for people and their data and increase greater acceptance of services that rely on data sharing and data use, it becomes increasingly important that the roles of the actors responsible for the protection of data be clearly defined, understood, and augmented. This paper thus, seeks to examine the role of these key actors in the data protection ecosystem by commencing with an introduction to the progressing role of data in the emerging world as well as its challenges, followed by a deep dive into the roles of the principal actors in the system in ensuring the protection of individuals and their personal data. The paper rounds off by concluding and making necessary recommendations for an effective promotion of the proper understanding of these duties by the actors across the ecosystem, without prejudice to innovative business practices.*

## INTRODUCTION

In recent years, collection of personal data has been carried out on a regular basis by different government agencies and corporations. A wide range of personal information is often shared in job applications, applications for driver's license, voter's card or in updating medical information. Businesses have taken advantage of this opportunity to forecast sales and staffing needs among other purposes. Private actors often rely on accurate, comprehensive public data collection to make smart decisions and to deal with the uncertainty surrounding the future demand for their products. Collectively, these well-informed decisions yield a stronger, more prosperous economy. Data collection by the government for the purpose of implementing better public policies is equally essential. Quality data at the disposal of policy makers reduces misuse of taxpayer funds and facilitates the exploitation of productive opportunities which will in turn



**Citation Information:** Apampa Olamilekan, S., (2024). The Expanding Significance of Data in the Emerging World: Assessing the Role of the Principal Actors in the Data Protection Ecosystem. *Journal of Legal, Ethical and Regulatory Issues, 27*(S1), 1-6.

develop the economy. However, despite this vast role of data in the contemporary world, cyber-attacks and data breaches is still a blooming underground industry, without prejudice to the substantial increase in cyber- security defence around the globe. A survey carried out by Statista has revealed that during the third quarter of 2022, approximately 15 million data records were exposed worldwide through databreaches. According to the survey, this figure had increased by 37 percent compared to the previous quarter. What is most intriguing is that when it comes to who we believe is most responsible for our data privacy – the government, corporations, or individuals – we cannot make up our minds. In reality, the response to this may differ greatly from one jurisdiction to another. The following section of this paper however examines the basic roles of the top line actors in the field in ensuring a sustainable widespread data protection ecosystem that could at best; keep up with the rapidly evolving information management climate. For ease of reference, these actors areclassified into two classes, viz – the state actors and the non-state actors.

## The State Actors

In the context of contemporary global data protection regimes, chief among the state actors in the system include the government of a given state, the data protection authority of the state and the court. These actors and their roles are discussed as follows

### The Government

As data and digital tools assume an expanding role in all aspects of our lives, it is significantly important to have clear and effective rules tailored to local realities and to support an even playing field to govern how different actors can use personal data through its life cycle and across different data ecosystems. The prime responsibilities of the government in ensuring the protection of individuals and their data includes the enactment of data protection laws that support useful innovations from both the public and private sectors, enforcement of actions to curb violations of the said laws, and requiring defaulting actors to rectify their unlawful actions by effectively implementing government-administered privacy and security programs. Beyond these, the government is also expected to ensure the funding, expertise, and political impetus needed to strengthen other actors in the system in order to enable them operate to the highest standard in their respective capacities**.**

### Data Protection Authority

Data Protection Authorities are often established by law. The authority acts as an independent, qualified and competent body of a state to oversee the implementation and due compliance by both public and private entities with the data protection laws of the state. They complement the work of other statutory institutions of the government in achieving the common goal of safeguarding the privacy of natural persons and collaborating with stakeholders in the system to foster safe conduct of transactions involving the exchange of personal data. As an organ of the state, they prevent manipulation of personal data and ensure that local and international businesses remain competitive through safe-guards afforded by a just and equitable legal regulatory framework on data protection, which is in tune with best practice. Furthermore, they promote public awareness of the risks, rules, safeguards, rights and obligations relating to processing. They advise the government and other institutions on legislative and administrative



**Citation Information:** Apampa Olamilekan, S., (2024). The Expanding Significance of Data in the Emerging World: Assessing the Role of the Principal Actors in the Data Protection Ecosystem. *Journal of Legal, Ethical and Regulatory Issues, 27*(S1), 1-6.

measures to ensure theprotection of personal data and they also handle complaints lodged by a data subject, or by a body.Where the law so empowers, they conduct investigations on the application of the state data protection law, encourage the establishment of data protection certification mechanisms and of data protection seals and marks, and monitor relevant developments, in so far as they have an impact on the protection of personal data.

## The Court

A court of law generally possesses the judicial authority to hear and adjudge disputes in civil andcriminal cases. Succinctly put, the role of the court in relation to data protection includes pronouncements on the rights of data subjects, giving appropriate orders and awarding damages as the circumstances of each case may deem fit. In a similar vein, it interprets the data privacy and other related laws of the state and allocates befitting meanings to them in cases of ambiguity. Furthermore, the court reviews decisions of administrative bodies in relation to data protection by examining the legitimacy of such decisions, that is, in terms of their fairness and adherence to the law. Similarly, in jurisdictions where judicial precedent is observed, the court develops the laws and sets precedence for deciding related cases in future.

## The Non-State Actors

Given the procedure and entities involved in the processing of personal data, the non-state actors in the ecosystem include Data Controllers, Data Processors and Data Subjects. These actors and their roles are as well discussed as follows.

## Data Controller

A Data Controller is the organization or the natural person which alone or with other persons, determines the purposes and means of processing personal data. The purposes and means are thereasons and modalities for collecting personal data. That is, which data is collected, why is it collected and what will it be used for? To identify the controller is to determine the actor(s) that determines this. In most privacy laws, the data controller has the most responsibility when it comes to protecting the privacy and right of the data subject. Generally, Data Controllers takes the responsibility of ensuring appropriate organizational and technical measures to protect data subject and their rights and equally demonstrate that they have implemented relevant data protection measures and processing principles institutionalized by the state. They may be required to take certain steps to secure data, such as encryption and pseudonymization, stability and uptime, backup and disasters recovery, and regular security testing.

Furthermore, data controllers maintain records of all processing activities; cooperate and consult with supervisory authorities in the performance of their tasks; and where applicable, appoint a dataprotection officer. They conduct data protection impact assessment where there is a chance that anew type of processing (especially when using a new technology) may cause a high risk to the rights and freedoms of natural persons. In the same vein, they notify the relevant authority in the event of a data breach and assist data subjects with exercising their rights to data privacy.



**Citation Information:** Apampa Olamilekan, S., (2024). The Expanding Significance of Data in the Emerging World: Assessing the Role of the Principal Actors in the Data Protection Ecosystem. *Journal of Legal, Ethical and Regulatory Issues, 27*(S1), 1-6.

## Data Processors

Processors are those engaged in processing personal data on behalf of the controller. The entity that operates the software the university uses to access and store its students' records would be theprocessor. Basically, processing is to be governed by a contract or other laws of the state that is binding on the processor. This contract or laws inter alia, determine certain obligations for the processors and how they assist the controller(s) fulfilling their roles and obligations. Data Processors thus act on the documented instruction of the controller with similar obligation as the controller. They ensure confidentiality, assist with legal compliance of the controller, respond to request from data subjects and make available, all information necessary to demonstrate the compliance of the controller. They take measures to assist the controller with ensuring security of processing, treat personal data after processing at the choice of the controller and ensure that each processing meets the requirements of the Law. Processors will also need to review existing data processing agreements to ensure that they have met their compliance obligations and inform the controller if something in the terms infringes on the privacy law.

## Data Protection Officer

The designation of Data Protection Officer (DPO) is an important measure and oftentimes a qualified requirement of the law to ensure legal compliance and protection of personal data. To keep up with compliance requirements, companies need data privacy and protection solutions thatgo beyond implementing security tools and monitoring traffic. They need a Data Protection Officerwho can take in the big picture view of the entire data ecosystem, map data flows, break down thedata protection specification that applies to them, help them stay complaint with data privacy laws and their updates, as well as pass all audits without any hiccups.

A DPO is an officer who monitors the application of and compliance with the data protection lawsof a state within an organization. Inter alia, the DPO informs and advices its organization on the data protection laws of the state and their related obligations. He monitors compliance with these laws and ensures that every member of the organization follows standard security and data protection practices by raising awareness, implementing a training process for all the members (including new employees) and monitoring of the organization security posture. A DPO has to device strategy to notify third parties and remote workers about sharing and processing of sensitive data and create a privacy governance ecosystem that eliminates all blind spots or vulnerabilities.[20] He provides advice on data breach management procedures and data protection impact assessment and monitors their performance. He promotes a security-aware culture across the organization, cooperates with the data protection authority and acts as a contact point for the authority on issue relating to processing and as well as the contact point for request from individuals regarding the processing of their personal data and the exercise of their rights.

## Data Subject

It is trite that, relatively, every human activity now generates a digital trace. From the forms he isasked to fill out, to the social media accounts he operates, to most of the technology he uses daily,each activity leaves a trail of his personal data behind. In order to give life to the letter of the



**Citation Information:** Apampa Olamilekan, S., (2024). The Expanding Significance of Data in the Emerging World: Assessing the Role of the Principal Actors in the Data Protection Ecosystem. *Journal of Legal, Ethical and Regulatory Issues, 27*(S1), 1-6.

law, a data subject beyond knowing the existence of its rights, needs to actively claim them. He needs to make use of his rights to bring a change in the behavior of the controller and processor as the public enforcement authorities cannot do it alone.

## CONCLUSION/RECOMMENDATION

The increasing digitization of government and business services, together with the fast-paced advancement in technology and the rapid development of the information management climate, have made it much easier to keep the most valuable element in this regard, which is personal data, in a digital format for easy duplication, transmission, and storage. With these commendable possibilities, what was formerly held under the lock and key and only available to a few became available and accessible online, consequently rendering it susceptible to different potential legal, tortuous and criminal activities from the public. What is the need to ensure the protection of thesedata against the backdrop of its increasing demand and the vast role it plays in the emerging worldif the key actors in the system lack adequate knowledge of their roles? Thus, it would suffice to say that enlightenment is crucial to enforcement and top performance. In light of this, it is recommended that, beyond the enactment and enforcement of comprehensive and market-driven privacy laws and policies by the state, effective frameworks for the enlightenment of these actorson the nitty-gritty of their roles in ensuring data privacy should be ensured at all levels across board. On a regular basis, they should be trained on the importance of their roles, their obligationsunder the law and the best ways to protect personal data. Data subjects should be educated on theimportance of their data, the measures to protect it and their privacy rights under the law.

Additionally, the content of the laws, the procedure for their implementation as well as the ethicsof responsibilities should all be appropriately taught to practicing professionals.

## REFERENCES

Daniella Balaban, "The roles and responsibilities of a Data Protection Officer" December 13, 2021

Data Privacy and Protection Regulations in Nigeria

In Order That They Might Rest Their Arguments on Facts: The Vital Role of Government-collected Data

Just like the European's General Data Protection Supervisory Authority (e.g, the Austrian Data Protection Authority); the Nigeria's Data Protection Bureau (NDPB) and the Ghana's Data Protection Commission (DPC) among other.

Number of data records exposed worldwide from 1st quarter 2020 to 1st quarter 2023(in millions)

Role Of Data Controller & Data Processor

What are the responsibilities of a data controller?

What are the responsibilities of a Data Protection Officer (DPO)?

**Received:** 27-Sept-2023, Manuscript No. JLERI-24-13915; **Editor assigned:** 29-Sept-2023, Pre QC No. JLERI-24-13915(PQ); **Reviewed:** 13-Oct-2023, QC No. JLERI-23-13915; **Revised:** 16-Oct-2023, Manuscript No. JLERI-23-13915(R); **Published:** 23-Oct-2023



**Citation Information:** Apampa Olamilekan, S., (2024). The Expanding Significance of Data in the Emerging World: Assessing the Role of the Principal Actors in the Data Protection Ecosystem. *Journal of Legal, Ethical and Regulatory Issues, 27*(S1), 1-6.