CLARIFYING THE DATA PROTECTION OBLIGATIONS OF CLOUD PROVIDERS AND CLOUD CUSTOMERS IN NIGERIA

It is generally assumed by some cloud customers in Nigeria that since they do not provide the cloud service, they have no compliance obligation if the cloud service is used to process the personal data of individuals in Nigeria. But as will be explained below, this is incorrect and not always the case according to the provision of the Nigerian Data Protection Regulations 2019 (NDPR) issued by the National Information Technology Development Agency (NITDA).

This short note is a consideration of the roles of cloud providers and cloud customers in the context of cloud computing, for the purpose of establishing their compliance obligations under the NDPR. To do this, this note examines the concepts of *data controller* and *processor*, and their data processing roles in a variety of cloud computing scenarios. These roles are assessed on a factual basis in which the cloud computing occurs and not necessarily based on parties' designation as provided in the terms of service (ToS) or other contractual arrangement between the cloud provider and cloud customer.

Of emphasis in this assessment is the unique definition of a data administrator/processor provided for in the NDPR which can be read broadly to include two categories of data processors, that is processors processing personal data on their own initiative and processors processing personal data on the initiative of a data controller. These categories of processors are for the purpose of this note referred to as, independent processors and controller-dependent processors respectively. As a result of this categorisation, it does appear that an independent processor is the same as a data controller and thus is subject to the same obligations imposed on a data controller under the NDPR.

Cloud Computing and Different Types of Cloud Business Models

Cloud computing is the provision of on-demand scalable computing resources and services over the internet according to user requirements. In this note, a user is the cloud customer, that is the person who has entered into a contractual arrangement to use a cloud service, while a cloud provider as the name implies is a person who has entered into a contractual arrangement to provide a cloud service.

These services could include software, infrastructure (i.e., servers), hosting and platforms (i.e., operating systems), and storage applications. Cloud computing has several applications from data storage, cloud gaming to email applications, and can be categorised as falling into one or more of the following business models;

i. **Infrastructure as a service** (IaaS), where the cloud provider provides remote access to and use of physical computing resources, and the cloud customer is responsible for implementing and maintaining both the operating platform and all applications.

ii. **Platform as a service** (PaaS), where the cloud provider provides access to and use of operating systems including related hardware, with the cloud customer responsible for implementing and maintaining the platforms and all the applications.

iii. **Software-as-a-service** (SaaS), where the cloud provider provision access to applications running on cloud infrastructure and accessible by a client interface.

Data Controller or Processor in a Cloud Environment

Under Art. 1.3 (g) of the NDPR a data controller is 'a person who either alone, jointly with other persons or in common with other persons or as a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed'. The reference to 'jointly' contemplates control by multiple persons since it is possible for different persons to be data controllers for the same set of personal data. In addition, and more importantly, key to this definition is the ability to decide how and for what purpose personal data is processed. In contrast, according to Art. 1.3 f) of the NDPR a data administrator (or processor as later clarified by NITDA) is a person or organisation that simply processes data. From this definition, it should be emphasized that unlike in other jurisdictions with data protection legislations, it is not expressly stated whether the data processor acts on behalf of the data controller, thus by implication the data processor may also be a controller in circumstances where it processes personal data on its own initiative. In other words, a data processor would be deemed to be a controller, and thus an independent processor only in circumstances where it decides 'how and for what purpose' personal data is to be processed. While, in circumstances where a data processor processes data only on the initiative or direction of the data controller, it is a controller-dependent processor and thus cannot be deemed to be a controller.

In processing data in a cloud environment, the cloud customer would most likely determine the ultimate purpose of the processing and if so, acts as the data controller. While the cloud provider if only providing the cloud service used for processing the data is assumed to be the processor. If such processing is done on the direction of the cloud customer who is also the data controller, then the processor is a controller-dependent processor. However, this does not negate the fact that the obligations of cloud providers and cloud customers in relation to the processing of personal data depends to a large extent on properly establishing which one of them is the data controller or data processor having regards to the circumstances of the data processing operation in the cloud environment. This in turn rests on a factual assessment of the particular cloud computing scenario, and not necessarily on the terms of services and/or contractual arrangement governing the relationship of the cloud provider and cloud customer. The clarification of these roles in a cloud environment is very important to correct the wrong assumption that cloud customers have no data compliance obligation if the cloud service is used for processing personal data. In fact, cloud customers have as much obligations as cloud providers, and in certain circumstances may even have more obligations under the NDPR.

For instance, in an IaaS scenario where the cloud customer uses cloud resources to run virtual machines to process data for various purposes, the cloud customer is the controller because it determines the purpose of the processing and means of processing by choosing the particular IaaS provider to use. In this scenario, the cloud provider remains a (controller-dependent) processor as long as it processes the data on behalf of, or on the instruction of the cloud customer. This is the same in a SaaS scenario where the cloud customer uses the SaaS applications for various data processing purposes, however if the cloud provider processes personal data outside the instruction of the cloud customer, for instance to improve the cloud service provided to a cloud customer's end users, the cloud provider will no longer be a (controller-dependent) processor but has automatically assumed the role of a controller (or an independent processor).

Obligations of Data Controller and Processor

The table below is a mapping of the various compliance obligations and their corresponding

provisions under the NDPR and which party is responsible for complying.

NDPR provisions	Brief description of compliance obligations	Controller and independent processor	Processor or controller-dependent processor
Art. 2.1	Compliance with the principles of lawful processing	✓	✓
Art. 2.2	Compliance with at least a ground for lawful processing	✓	✓
Art. 2.5	Displaying a privacy policy in a conspicuous place	✓	✓
Art. 2.6	Implement appropriate data security measure(s)	✓	✓
Art. 2.7	Obligation to enter into a third-party processing contract when engaging a third-party to process data	✓	
Art. 2.11	Compliance with the conditions for transfer of data to a foreign country or international organisation	✓	
Art. 2.13	Give effect to, and facilitate the exercise of the rights of the data subject	✓	
Art. 3.1	Making available data protection policy to the general public	✓	
Art. 3.1.2	Designation of Data Protection Officer (DPO)	✓	✓
Art. 3.1.3	Ensuring continuous training for DPO	✓	✓
Art. 3.5	Conducting a data protection audit	✓	✓

As can be seen in the table above, only four obligations are not mandatory for the data processor or controller-dependent processor, while the controller and independent controller are obligated to comply with all eleven of them. In other words, if it is established in a cloud environment that the cloud customer is the data controller and the cloud provider is the data processor, then the cloud customer is obligated to comply with all the eleven obligations applicable to a data controller as would the cloud provider be obligated to comply with only the seven obligations applicable to data processors under the NDPR. However, it bears emphasis to mention that the above stated obligations are only in respect of those provided for in the NDPR as other data compliance obligations provided for in other regulatory frameworks may also apply.

Conclusion

This note is a first level screening to identify who is responsible for what under the NDPR, as the concept of data controllers and processors may not be easily established in a complex cloud environment where different parties have varying degrees of influence over how data is processed and for what purpose, without an in-depth analysis of the particular data processing operation. An in-depth analysis would also be required to establish the existence of pluralistic control where the cloud provider and cloud customer can both be characterised as 'jointly' determining the purpose and manner of the data processing operation, and thereby are bound to comply with the applicable obligations under the NDPR.

The adoption of cloud services continues to rise as evidenced by several impressive statistics, some of which are; global cloud spend will grow to $500 Billion by 2023, an estimated 80% of all companies in the world will be using cloud services by the end of 2021, using cloud services over traditional servers can

cut a company's IT cost by up to 65%, some companies claim that they've seen increased profits up to 28% from using cloud services, every 0.5 second an IT service is delivered through the cloud and even back to Nigeria where the market was recently stated to be worth about $500 million annually. All these underscores the importance of cloud computing to a thriving digital economy and is indeed mentioned in two of the eight pillars required for the acceleration of Nigeria's digital economy pursuant to the National Digital Economy Policy and Strategy. For this market to remain competitive whilst delivering on its value proposition regarding cost, flexibility and efficiency, it is very important that cloud services are trustworthy, particularly with respect to assurances and safeguards that data entrusted to cloud providers are utilised in manner that complies with the requirements of existing laws including the applicable data protection regime.

Disclaimer

Contact person for this Article
Chukwuyere Izuogu
Senior Associate
chukwuyere@sskohn.com

Contact us at:
16D Akin Olugbade Street
(Off Adeola Odeku Street)
Victoria Island, Lagos
Tel: +234 1 271 2276; **Fax:** +234 1 271 2277
Email: info@sskohn.com; **Website:** www.sskohn.com