Introduction

In today's digital world, almost all organisations rely on third parties for processing personal data. Processing is defined by the Nigerian Data Protection Regulation, 2019 (the Regulation) as follows:

> *"any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*[1]

The Regulation requires data processing by third party to be governed by a written contract between the third party and the Data Controller.[2] The written contract referred to is called a Data Processing Agreement (DPA) which is between the organisation (the Data Controller) and any party that acts as a data processor on their behalf.

This paper provides a brief description of the concepts of controller and processor, what are DPAs, are they really necessary for you, what do they look like, and who needs to be involved from within your organisation?

Controller and Processor

The data protection concepts will help organisations determine whether they are subject to the Regulation in any given instance, what role they are playing in a transaction (controller or processor), any where to look for additional guidance on Regulation compliance. The definitions of controller and processor are key to determining the allocation of legal obligations which may arise under data protection regulations or law. It is essential for protecting the rights and freedoms of data subjects. A data controller means a person who either alone, or jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed.[3] The data controller is the key decision maker with regards personal data. Therefore, most of the responsibilities for compliance with the

1 Nigerian Data Protection Regulation 2019, Article 1.3(xxi)
2 Nigerian Data Protection Regulation 2019, Article 2.7
3 Nigerian Data Protection Regulation 2019, Article 1.3(x)

Regulation fall on the data controller's shoulders. The data controller determines the purpose for which personal data is being collected, stored, used, altered and disclosed.

Data processor or administrator means a person or organisation that processes data.[4] The General Data Protection Regulation (GDPR) defines a processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[5] The data processor is required by the DPA to process personal data only on instructions of the Data Controller. The EU General Data Protection Regulation (GDPR) GDPR requires that the processor processes personal data only on the controller's instructions and that a contact or a binding legal act regulating the relations set out the nature and purpose of any data processing, the type of personal data and the categories of data subjects.

The GDPR also requires that the processor processes personal data only on the controller's instructions and that a contract or a binding legal act regulating the relations between the controller and the processor be put in writing.[6] The contract must expressly set out the nature and purpose of any data processing, the type of personal data and the categories of data subjects.[7]

The contract between the controller and the processor is an essential element of their relationship, and is a legal requirement.[8] For example: The director of the Sunshine Company decides that the Cloudy Company – a specialist in cloud-based data storage – should manage Sunshine's customer data. The Sunshine Company remains the controller and Cloudy Company is only a processor, as, according to the contract, Cloudy may only use Sunshine company's customer data for the purposes that Sunshine determines.[9]

Definition of a Data Processing Agreement (DPA)

A DPA is a written agreement between an organisation (data controller) and a third-party organisation (data processor) that ensures that all processing tasks are carried out in accordance with both the data protection regulations of the country and the data controller's instructions.

The Regulation does not provide a definition, however the GDPR defines a DPA as a legally binding document to be entered into between the data controller and the data processor, either

4 Article 1.3(ix) NDPR
5 General Data Protection Regulation (GDRP), Article 4(8)
6 European Data Protection, Law and Practice 2nd Edition pg. 86
7 Article 28 GDPR sets out detailed content for the processing contract.
8 Ibid., Art. 28 (3)
9 Handbook on European Data Protection, pg.108

in writing or electronic form. The DPA acts as an agreement that clarifies the responsibilities, obligations, and clauses for all involved parties to act upon.

The main parties involved in signing a DPA are of course the data controller and data processors. In addition, there may be two or more controllers who jointly determine the purposes and means of processing. Also, the complex structures of modern outsourcing may mean that a controller's subcontracts processing operations to more than one processor or a data processor subcontracts the processing operations totally or partially to two or more subcontractors.[10] Therefore, every other party involved in the processing of your organisation's data should also be included in the DPA. For example, your organisation has outsourced human resources to company A, but company A outsources the recruitment responsibilities within their task to company B. Company C then becomes a sub-processor, and both company A and B would be required to sign a DPA with your organisation. Every party that plays a role must be well informed of their duties, and will have the same legal obligations towards the Regulation compliance as the 'original processor'.

Contents of a Standard DPA

The Regulation does not provide detailed content for the DPA. However, Article 2.7 of the Regulation provides that any person engaging a third party to process the data obtained from data subjects shall ensure adherence to this Regulation. Accordingly, Article 2.4(b) of the NDPR provides:

> *"A party to any data processing contract, other than an individual data subject, shall take reasonable measures to ensure the other party does not have a record of violating the principles set out in Section 5 and he is accountable to NITDA or a reputable regulatory authority for data protection within or outside Nigeria; accordingly, every Data Processor or Controller shall be liable for the actions or inactions of third parties which handles the personal data of Data Subjects under this Regulation."*

This provides a general idea in respect of the contents of a DPA in compliance with the NDPR. However, the GDPR sets out key points that should definitely be included in a DPA:

- The data processor agrees to process personal data only on documented instructions provided by the data controller.

[10] European Data Protection Law and Practice 2nd Edition pg. 87

- Every individual that works with the personal data is sworn to confidentiality.
- That adequate technical and organisational measures are taken to ensure the security of the data.
- The data processor agrees to not subcontract to another processor unless clearly instructed to do so in writing by the controller.
- The data processor agrees to help the data controller in upholding their obligations under the GDPR, especially surrounding the data subject's rights.
- That the data processor agrees to aid the data controller in maintaining appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests to exercise the data subjects' rights.
- The data processor agrees to erase all personal data or return the data to the controller, upon a termination of services.\The processor will assist the controller in complying with the its' obligations (security, data protection impact assessment and breach notification), taking into account the nature of the processing.
- That the data processor must allow the controller to carry out an audit, and will provide information necessary to prove compliance.[11]

The above key points will provide your organisation and the parties involved the opportunity to clarify what is expected and how to carry out tasks. Additionally, these points also provide room for your organisation to identify potential problems and rethink procedures.

Sample DPA

An example situation where a DPA is required between a data controller and a processor.

An organisation engages the services of a pension scheme administrator to handle the pension schemes of its employees. The organisation is the data controller while the pension scheme is the data processor. However, where the pension scheme administrator is using the details of its pension scheme members to market its other financial products it shall also be considered to be a data controller in respect of that processing. A DPA is required between the organisation and

[11] EU General Data Protection Regulation, Article 28

the pension scheme administrator, which needs to include the responsibilities that explain the handling of user requests or contact forms. The DPA may cover:

- Definitions of terms that are referred to in the DPA;
- The type(s) of personal data that will be processed and categorised;
- Overview of obligations between the data controller and data processor;
- The different types of personal data and information received from the employees and how it's categorised;
- The categories of data subjects;
- The length of time that personal data are kept and the duration of time processing is carried out;
- Details on data encryption and other security measures; and
- Obligations and responsibilities of each party in the event of a data breach.

Conclusion

The DPA can be a lengthy document to create that can require quite a bit of preparatory work like data mapping, Data Protection Impact Assessments (DPIA), time investment, and resources. DPAs are crucial role in compliance with the Regulation and GDPR. It ensures that all duties are appropriately aligned with the Regulation. DPAs will assist organisations to further improve procedures and security initiatives over data handling, even reduce the risk of a data breach or incident, and increase accountability and efficiency.

For further information on this topic, please contact Nouvelle Legal by telephone (+2349097809000), or e-mail yketiku@nouvellelegal.com)

Nouvelle Legal website can be accessed at www.nouvellelegal.com.com