THE APPLICATION OF EU'S GENERAL DATA PROTECTION REGULATIONS TO ORGANIZATIONS LOCATED IN NIGERIA

Recently, Chukwuyere Ebere Izuogu, Senior Associate at Streamsowers & Köhn, participated in a Google sponsored seminar on Data Privacy and Security convened by the African Academic Network on Internet Policy at the Ibadan School of Government and Public Policy. At the seminar, he spoke about the state of personal data protection in Nigeria. As would be expected, an emergent issue repeatedly debated (and hotly too) during this seminar is the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which is expected to become effective from 25 May 2018 across member states of the EU, and its extra-territorial reach to organizations outside the EU. This work will examine GDPR and the principles and grounds for processing personal data under the GDPR. It will also consider issues such as how organizations located in Nigeria may come within the scope of application of the GDPR, how the obligations imposed by the GDPR and the penalties for non-compliance with these obligations. Finally, it will offer a practical advice on how compliance with the GDPR may be commenced by such organizations.

WHAT IS THE GDPR?

The GDPR is an EU wide personal data protection regime. The GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data within the EU area (Article 1 (1)). Under the GDPR, personal data is any information which directly establishes the identity of a natural person (who is the data subject), or when combined with other pieces of information will allow such an individual to be identified, examples of personal data are personal names, facial photographs, IP addresses, residential addresses and finger prints. Processing on the other hand means "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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4 (2)). In addition, two different categories of organizations process personal data under the GDPR and they are; "controllers" and "processors". A controller, acting alone or together with others, "determines the purposes and means of the processing of personal data" (Article 4 (7)). A processor, on the other hand, "processes personal data on behalf of the controller" (Article 7 (8)).

The GDPR will replace the extant Data Protection Directive (Directive 95/46/EC) which has been in force since 1995. As at the time of this writing, the GDPR is the world's most detailed data protection law.

WHAT ARE THE PRINCIPLES AND GROUNDS FOR PROCESSING PERSONAL DATA UNDER THE GDPR?

These are the conditions that must be satisfied before personal data can be lawfully processed under the GDPR. These conditions are:

I. Fair and lawful processing (Article 5 (1) (a))

In EU legal interpretation, the satisfaction of this principle is achieved if the processing of personal data is in accordance with the law, pursues a legitimate purpose, and is necessary in a democratic society in order to achieve the legitimate purpose. Thus, the processing of personal data is in accordance with the law if it based on the provision of a law; pursues a legitimate aim if it is consistent with a named public interest or the rights and freedoms of others; and necessary in a democratic society if it "corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued".

II. Purpose limitation (Article 5 (1) (b))
According to this principle, the purpose for which personal data is processed must be stated clearly, at a time no later than when the data is collected. Thus, processing of personal data for an undefined and/or unlimited purpose is unlawful or will have no legal basis, unless the consent of the data subject is first obtained or that such additional processing is by authority of law.

III. Data minimization (Article 5 (1) (c))
According to this principle, the data controller should limit the processing and/or collection of personal data to that which is directly relevant for achieving the specific purpose for which the data is collected or processed.

IV. Accuracy (Article 5 (1) (d))
This principle requires that a data controller holding personal data shall not use that information without taking steps to ensure with reasonable certainty that the data are accurate and up to date.

V. Retention (Article 5 (1) (e))
This principle requires that personal data be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

VI. Data security (Article 5 (1) (f))
This principle requires that the data processing operation adopt security measures that safeguards the confidentiality, integrity and availability of the personal data processed, and the systems used for processing them.

WHICH ORGANIZATIONS LOCATED IN NIGERIA ARE SUBJECT TO THE GDPR?

Article 3 of the GDPR sets out the territorial scope of the GDPR. In this regard, organizations located in Nigeria acting as data controllers and/or data processors would be subject to the GDPR in any of the following circumstances:

I. Where the organization maintains an "establishment" in the EU and processes personal data "in the context of the activities of [that] establishment, regardless of whether the processing takes place in the EU or not" (Article 3 (1)). Establishment in this context implies "the effective and real exercise of activity through stable arrangements" (Recital 22). Thus, an organization located in Nigeria with a branch or subsidiary in the EU would be caught by this provision if it processes personal data in the context of that establishment.

II. Where the organization processes personal data with respect to "the offering of goods or services, irrespective of whether a payment is required, to data subjects in the [EU]" (Article 3 (2) (a)). Whether a controller or processor is offering goods or services to data subjects in the EU, depends on the consideration of such factors as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the

mentioning of customers or users who are in the EU, and not on the mere accessibility of the controller's or processor's website in the EU, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, (Recital 23). Thus, the GDPR will be triggered once it can be established that an organization located in Nigeria processes personal data in respect of the offering goods or services to data subjects located in any part of the EU.

III. Where the organization processes personal data in context of the monitoring of the behaviour of data subjects in the EU as far as their behaviour takes place within the EU (Article 3 (2) (b)). For instance, the GDPR would be triggered where natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes by organizations located in Nigeria.

WHAT ARE THE OBLIGATIONS IMPOSED BY THE GDPR ON SUCH ORGANIZATIONS?

In addition to complying with the principles for processing personal data, any organization that falls into any of the foregoing three categories is required to comply with the following obligations:

I. Information and access rights of data subject:

The data controller is required by Article 13 (1) of the GDPR to provide certain types of information to the data subject at the time of collecting personal data.

II. Rectification and erasure right of the data subject:

Article 16 of the GDPR requires the data controller to allow the data subject to correct inaccurate aspects of his personal data. In addition, Article 17 of the GDPR obligates the data controller in certain circumstances to erase the personal data of the data subject, upon the request of the data subject.

III. Data portability:

Under certain conditions, Article 20 of the GDPR obligates the data controller to provide the data subject's personal data in a machine-readable format or transmit same to another controller, upon request by the data subject.

IV. Data protection by design and default:

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects (Article 25 (1)).

V. Appointment of a designated representative:

A data controller or processor not established in the EU but subject to the GDPR is required

by Article 27 to designate a representative in the EU.

VI. **Data breach notification:**
The data controller is obligated by Article 33 (1) of the GDPR to notify a personal data protection breach to the competent supervisory authority within 72 hours of becoming aware of it. An exception to this is where the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

VII. **Data protection impact assessment:**
Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Article 35 (1)).

VIII. **Appointment of a data protection officer:**
Article 37 requires both the data processor and controller to appoint a data protection officer in particular circumstances.

WHAT ARE THE PENALTIES FOR FAILURE TO COMPLY WITH THE GDPR?

Depending on the particular provision of the GDPR a data controller or processor fails to comply with, it could be potentially liable to the payment of an administrative fine of up to 10, 000, 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher; or administrative fines up to 20, 000, 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, a person who has suffered a material or non-material damage resulting from the failure to comply with an obligation imposed by the GDPR is entitled to a compensation.

CONCLUSION

Now that the GDPR is upon us, organizations in order not to risk enforcement actions by the competent supervisory authority must ensure that their activities are consistent with the GDPR. The first step in this complex process is to ascertain whether its activities (or any aspect of it) indeed comes within the reach of the GDPR, and if necessary, commence steps to mitigate its exposure to liability under the GDPR.

In the context of cross-border transfer of personal data from the EU, data controller or processor organizations in Nigeria may need to consider implementing safeguards such as a legally binding enforceable instrument, data protection by contractual clauses and/or a certification mechanism.

As 25 May 2018 draws near, the global data protection ecosystem eagerly awaits the far-reaching revolutionary changes coming in the wake of the GDPR.

Chukwuyere is a Senior Associate at Streamsowers & Köhn and the author of "Regulating Anti-Competitive Practices in Nigeria's Communications Sector" (Oisterwijk, Netherlands: Wolf Legal Publishers, 2017).

Disclaimer: This article does not constitute legal advice neither is it a substitute for obtaining legal advice from a legal practitioner.

info@sskohn.com; chukwuyere@sskohn.com