THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATIONS AND ITS IMPACTS IN NIGERIAN BUSINESSES

Introduction:

The cross border nature of the internet has made it difficult to confine data processing to a specific geographical border. In attestation to this fact, the National Information Technology Data Agency (NITDA)[1] like the Biblical John the Baptist, forewarned Nigerians on the probable impact of the forthcoming European Union (EU) General Data Protection Regulation on Nigerian businesses[2] which according to Techpoint Africa, will include airlines, banks, hotels, fintech companies, digital advertising agencies amongst others.[3] Three months later, the EU implemented the Regulation on the protection of natural persons with regards to the processing of personal data and on the free movement of such data. A landmark regulation that has been hailed as one of the legacies of the century and on the flipside has been jested to be as broad enough to cover Sancta Claus. In a year since the adoption of the GDPR, European data protection agencies have issued fines totaling –56 million from more than 200,000 reported cases[4]. With the GDPR's emphasis on strict compliance and its punitive sanctions it is safe to observe its provisions and find out if its long arms were wide enough to embrace Nigerian businesses.

Brief History

The GDPR repealed the Data Protection Directive (DPD) of 1995 which although was successful, faced the hurdle of fragmentation and expensive administrative measures across its member states.[5]Then, in 2012, the EU proposed a comprehensive reform of data protection rules in the EU. Two decades after the1995 was made, the 28 states comprising the EU adopted the Regulation on the protection of natural persons with regards to the processing of personal data and on the free movement of such data which was implemented on the 25th of May 2018.

What is personal data?

Personal data is defined broadly under the GDPR to mean any information relating to an identified or identifiable natural person (referred to as the data subject) who can be identified

---

[1] An Agency of the Nigerian government created to implement the Nigerian Information Technology Policy and co-ordinate the general Information technology development and regulation in the country.

[2] Drusman, NITDA Alerts Nigerians on European Union's General Data Protection Regulation Implementation and Enforcement, NITDA News (June 26 2018) <https://nitda.gov.ng/nit/nitda-alerts-nigerians-on-european-union-general-data-protection-regulation-implementation-and-enforcement-2/ >accessed 13 March 2019.

[3] Enyioma Madubike, The GDPR-7 types of Nigerian companies that should comply, (May 21 2018) Techpoint website <https:?/techpoint.africa/2018/05/31/gdpr-compliance-nigeria/> accessed on 14 March 2019.

[4] Rebecca Hill, Year 1 of GDPR: Over 200,000 cases reported, firms fined €56 meeelli.. Oh, that's mostly Google (March 12 2019) The Register website <https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/> accessed on the 14th March 2019.

[5] K. Paisley, It's all about data: the impact of the EU General Data Protection Regulation on international arbitration, Fordham International Law Journal (2018) Vol41,Isssue 4, Article 4 *pg.* 850.

directly or indirectly, in particular by reference to an identifier[6] such as a name, an identification number, location data or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This means that all business-related information exchanged during a typical business relationship containing information by which a person can be identified is personal data under the GDPR.

Territorial scope of the GDPR

The GDPR will apply to;

- **The processing of personal data in the context of the activitiesof an establishment of a controller[7] or a processor[8] in the EU regardless of whether the processing takes place in the EU or not[9].**

Although, this provision generally applies to controllers and processors in the EU, the decision of the Court of Justice of the European Union (CJEU) in the case of Google Spain SL v. Agacia Espanola de Proteccion de Datus[10] extended its application when it held that the data processing status of the search engine – although not carried out by Google Spain subsidiary were sufficiently connected with the Spanish entity so as to be considered established in Spain for the purposes of the Directive.

Thus, this would impact corporate groups that have operations in both Europe and Nigeria if personal data that is relevant to the European business is processed in Nigeria.

- **Where the Nigerian company processes the personal data of persons who are in the EU where the processing activity is related to the offering of goods or services (whether free or paid for) to such subjects in the EU.**

  The yardstick for determining whether a Nigerian company is offering goods and services to data subjects who are in theEU is "*whether the Nigerian company envisages offering its products to individuals in the EU".*[11]

  Inorder to determine whether the Nigerian company envisages offering its products to individuals in the EU, the fact that it uses European language or currency to order goods and services and that it makes reference to customers in the EU may be considered.

- **Where the Nigerian company processes personal data of subjects who are in the EU where the processing activity is related to the monitoring of their behavior as far as their behavior takes place in the EU**.

---

[6] Internet Protocol addresses, cookies, MAC addresses and Radio Frequency Identification tags have been considered personal data.
[7] A Person or an entity that determines how and what to use information for. The data controller is accountable for compliance and keeps records of decisions made for the protection of personal data. But, these requirements do not apply to small and medium-sized enterprises (SME's) having less than 250 employees although they would still need to demonstrate compliance.
[8] Persons or entities who may be engaged by a controller to process data on their behalf such as an agent or a supplier.
[9] Article 3(1).
[10] Case C-131/12 ILEC 060 (CJEU 2014).Google Spain. The CJEU stated this while construing article 4(1) of the directive, the equivalent of Article 3(1) of the GDPR
[11] The CJEU decided in the Pammer case (C-585/08 and C-144/09) that the mere accessibility of a trader/intermediary/controller's website or email address or contact details in a member state is not sufficient to ascertain such intention.

A Nigerian company that tracks data subjects on the internet through personal data techniques such as profiling or through the use of targeted cookies in order to take decisions concerning them, analyzing or predicting their preferences behaviors and attitudes will be included in this provision.

How Nigerian businesses can be compliant to the EU GDPR

1. **By appointing a representative**; who must be located in one of the European countries of the individuals who are offered products or are subject to behavioral monitoring. [12]
2. **Data audit**; this involves assessing all data processing activities likely to involve processing of personal data of individuals in the EU
3. **Reviewing consent**; Nigerian businesses will need to elicit specific consent from customers before their data is processed.
4. **Update data privacy notice** in line with global outlook to ensure regulatory compliance.
5. **By ensuring data subject right;** The rights are- right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability,and the right to object to the processing of personal data.
6. By training their workers on GDPR compliance
7. By employing the use of pseudonymized or anonymised data to protect personal data[13]
8. By considering appropriate insurance coverage where the business processes data on a large scale

Transfer of Personal Data to Third Countries (Nigeria)

The GDPR has recognized the necessity for data transfers to non EU countries and have prescribed the conditions under which such data may be sent. They are;

- Where the EU has some international data transfer agreement with such third country
- Where the European Commission approves a third country as having adequate degree of protection for personal data in their jurisdiction known as; *Adequacy decisions*.[14]Before the Adequacy Decision is made, the third country's data protection practices should be as strong as the GDPR, and be backed by appropriate laws and regulations enforced by a cooperative supervisory authority and operate within a democratic legal framework that allows individuals to enjoy their data rights.
- Where the Controller or processor puts in place appropriate Safeguards.
  This will suffice where a country has not been deemed adequate by the European Commission for the transfer of personal data. The controller or processor can employ following safeguards;

[12] Where the data processing activities are occasional and does not involve large scale processing of special categories of data such as personal data revealing race, ethnicity, origin, political opinions, beliefs, health records, genetic or biometric data, or criminal records and unlikely to result in a risk to the rights and freedom of individuals, the non EU entity would be exempted from appointing a representative.
[13]Recital 28.
[14] Applying this, on 30th September 2018, the EU had given approval for free transfer of data to 12 nations that have signed the Privacy Shield- Andorra, Argentina, Canada, Israel, United States of America, New Zealand, Faroe Island, Isle of Man, Switzerland, Uruguay, Guernsey, Jersey and Japan.

Binding corporate rules; Which establish a binding code of conduct for a group of companies engaged in a joint economic activity that they will comply with a set of data protection rules
Standard data protection clauses; These are issued by a supervisory authority or by the European Commission
Adoption of standard contractual clauses; that has previously be approved by the European Commissionto be inserted into contracts[15]
Binding commitments to adhere to approved codes of conduct or certifications
Ad hoc contractual engagement between the EU transferor and third country recipient of the data that has been approved by a concerned supervisory authority.

Exceptions to Third Country Transfers

The rules on international transfer of data[16]could be waived in the following situations;

- where a person has explicitly consented to the transfer.
- where the transfer is necessary for the performance of a contract between the data subject and the controller.
- Where the transfer is required for the fulfillment of a contract in the interest of the data subject between the controller and another legal person.
- Where the transfer is necessary on grounds of public interest.
- Where the transfer is required in relation to a legal or regulatory claim.
- Where the transfer is necessary in order to protect the vital interests of the data subject or other persons where the data subject cannot give consent.
- Where the transfer is made from a public register.

Also the GDPR also makes reservations for transfer of personal data to data subjects where it is necessary for the compelling legitimate interest of the controller which does not override the legitimate interest of the data subject where the transfer is not repetitive, concerns a limited number of data subjects and has informed them of such transfer, and has provided suitable safeguards for the protection of the personal data and has informed the supervisory authority.[17]

Breach

Noncompliance with the GDPR attracts a sanction of up to 4% annual worldwide turnover of an organization or E20 million for the most serious violations and half of it for less serious violations. Also, data subjects have the right of enforcement before courts and regulatory authorities to obtain damages. And there is the possibility of criminal sanctions. Although the

[15] Document number C(2004)5271) (2004/915/EC) Commission Decision (27Decembner 2004)< https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915> accessed on March 14 2019.
[16]Such as adequacy decision and use of safeguards.
[17] Article 49.

challenge of enforcement as to how the GDPR will be enforced in third countries still raises its head.

The Nigerian Data Protection Regulation

Nigerian Data protection Regulation became operational on the 25th of January 2019. Although, the regulation tried to make its provisions in tune with global best practices, through its provisions on rights of data subjects, procedure for data transfers and processes, it has also been criticized as not being as comprehensive and extensive as the EU GDPR by its failure to provide for the protection of sensitive personal data, prohibition of processing or the permissible exceptions to process data and the absence of legitimate interest as a legal basis to process data.[18] Hence, Nigerian businesses that fall within the scope of the GDPR would have to comply with the provisions of the GDPR as the existence of the Nigerian Data Protection Regulation does not exclude the application of the GDPR in Nigerian businesses.

Conclusion

Although the question of enforceability of the EU GDPR in non EU entities continues to rear its head, it has been conceded that its Nigerian businesses that have subsidiaries in the EU that may be mostly affected by the provisions of the EU GDPR. However considering the steep fines imposed by the GDPR for non-compliance with its provisions, it is imperative for all Nigerian businesses with European affiliates, counterparts, and clients to ensure effective data protection strategies through updating its privacy notices, data handling policies and updating its contract clauses, ensure the rights of data subjects, and where the business processes large data seek out insurance coverage.

[18] Ridwan Oloyede, NITDA Protection Regulation 2019: building trust responsibly (March 17 2019) <https://www.lexology.com/library/detail.aspx?g>accessed on March 15 2019